ЛЕКЦИИ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ
И ТЕОРИИ АЛГОРИТМОВ

Н. К. Верещагин, А. Шень

НАЧАЛА ТЕОРИИ МНОЖЕСТВ

Издание четвёртое, дополненное

Москва
Издательство МЦНМО, 2012

УДК 510.22
ББК 22.12
В31

Верещагин Н. К., Шень А.

В31 Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств. — 4-е изд., доп. — М.: МЦНМО, 2012. — 112 с.

ISBN 978-5-4439-0012-4

Книга написана по материалам лекций и семинаров, проводившихся авторами для студентов младших курсов мехмата МГУ. В ней рассказывается об основных понятиях «наивной теории множеств» (мощности, упорядоченные множества, трансфинитная индукция, ординалы). Изложение рассчитано на учеников математических школ, студентов-математиков и всех интересующихся основами теории множеств. Книга включает около 150 задач различной трудности.

Предыдущее издание книги вышло в 2008 г.

ББК 22.12

Николай Константинович Верещагин
Александр Шень

Лекции по математической логике и теории алгоритмов.
Часть 1. Начала теории множеств.

Подписано в печать 11.04.2012 г. Формат 60 × 90 1/16. Бумага офсетная.
Печать офсетная. Печ. л. 7. Тираж 1000 экз. Заказ №

Издательство Московского центра
непрерывного математического образования.
119002, Москва, Б. Власьевский пер., 11. Тел. (499) 241–74–83.

Отпечатано с готовых диапозитивов в ППП «Типография „Наука“».
121099, Москва, Шубинский пер., 6.

ISBN 978-5-4439-0012-4

Оглавление

Предисловие

Предлагаемая вашему вниманию книга написана по материалам лекций для младшекурсников, которые читались авторами в разные годы на механико-математическом факультете МГУ. (В эту же серию входят книги «Языки и исчисления» и «Вычислимые функции».)

Основные понятия теории множеств (мощности, трансфинитная индукция, ординалы) входят в число вещей, которые хорошо бы знать любому грамотному математику (даже если он не является математическим логиком или общим топологом). Обычно про них коротко пишут в первых главах учебников анализа, алгебры или топологии, спеша перейти к основной теме книги. А жаль — предмет достаточно интересен, важен и прост, чтобы рассказать о нём не торопясь.

Именно такой популярный рассказ мы пытались написать, имея в виду самых разных читателей: от подготовленного школьника (захотевшего перейти от побед на олимпиадах к чему-то более осмысленному) до профессионального математика (решившего прочитать по дороге на отдых, что же такое трансфинитная индукция, которую всегда заменяют леммой Цорна). Для более подробного знакомства с теорией множеств читатель может обратиться к другим книгам (некоторые из них перечислены в списке литературы на с. 105).

Авторы пользуются случаем поблагодарить своего учителя, Владимира Андреевича Успенского, лекции, тексты и высказывания которого повлияли на них (и на содержание этой книги), вероятно, даже в большей степени, чем авторы это осознают.

При подготовке текста использованы записи А. Евфимьевского и А. Ромащенко (который также прочёл предварительный вариант книги и нашёл там немало ошибок).

Оригинал-макет книги был подготовлен В. В. Шуваловым; без его настойчивости (вплоть до готовности разделить ответственность за ошибки) оригинал-макет вряд ли появился бы к какому-либо сроку.

Авторы признательны École Normale Supérieure de Lyon (Франция) за поддержку и гостеприимство во время написания этой книги.

Первое издание книги стало возможным благодаря Российскому фонду фундаментальных исследований, а также И. В. Ященко, который уговорил авторов подать туда заявку.

Наконец, мы благодарим сотрудников, аспирантов и студентов

кафедры математической логики мехмата МГУ, а также всех участников наших лекций и семинаров и читателей предварительных вариантов этой книги.

Просим сообщать о всех ошибках и опечатках авторам (электронные адреса `ver` at `mccme` dot `ru`, `nikolay` dot `vereshchagin` at `gmail` dot `com`; `sasha` dot `shen` at `gmail` dot `com`, `alexander` dot `shen` at `lirmm` dot `fr`; почтовый адрес: Москва, 119002, Большой Власьевский пер., 11, Московский центр непрерывного математического образования).

Во втором издании исправлено несколько ошибок и добавлено несколько новых задач. В третьем издании был дополнен именной указатель и восстановлен предметный указатель. пропущенный во втором издании по вине авторов. В четвёртом издании (помимо изменения формата вёрстки и использования шрифтов LH) сделаны небольшие добавления, в основном связанные с аксиомой выбора.

Н. К. Верещагин, А. Шень

1. Множества и мощности

1.1. Множества

Основные понятия и обозначения, связанные с множествами и операциями над ними:

- *Множества* состоят из *элементов*. Запись $x \in M$ означает, что x является элементом множества M.

- Говорят, что множество A является *подмножеством* множества B (запись: $A \subset B$), если все элементы A являются элементами B.

- Множества A и B *равны* (запись: $A = B$), если они содержат одни и те же элементы (другими словами, если $A \subset B$ и $B \subset A$).

- Если A — подмножество B, не равное всему B, то A называют *собственным* подмножеством B (запись: $A \subsetneq B$).

- *Пустое* множество $\varnothing$ не содержит ни одного элемента и является подмножеством любого множества.

- *Пересечение* $A \cap B$ двух множеств A и B состоит из элементов, которые принадлежат обоим множествам A и B. Это записывают так:
$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}$$
(читается: множество таких x, что ...).

- *Объединение* $A \cup B$ состоит из элементов, которые принадлежат хотя бы одному из множеств A и B:
$$A \cup B = \{x \mid x \in A \text{ или } x \in B\}.$$

- *Разность* $A \setminus B$ состоит из элементов, которые принадлежат A, но не принадлежат B:
$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}.$$
Если множество B является подмножеством множества A, разность $A \setminus B$ называют также *дополнением B до A*.

- *Симметрическая разность* $A \triangle B$ состоит из элементов, которые принадлежат ровно одному из множеств A и B:

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

- Через $\{a, b, c\}$ обозначается множество, которое содержит элементы a, b, c и не содержит других. Если среди a, b, c есть равные, оно может содержать один или два элемента. Подобное обозначение используется и в менее формальных ситуациях: множество членов последовательности $a_0, a_1, \ldots$ обозначается $\{a_0, a_1, \ldots\}$ или даже $\{a_i\}$. Более аккуратная запись для того же множества такова: $\{a_i \mid i \in \mathbb{N}\}$, где $\mathbb{N}$ — множество натуральных чисел $\{0, 1, 2, \ldots\}$.

Понятие множества появилось в математике сравнительно недавно, в конце 19-го века, в связи с работами Кантора (сравнение мощностей множеств), о которых пойдёт речь дальше (раздел 1.3 и следующие). Некоторое время назад этот язык пытались внедрить в школьное преподавание, объясняя ученикам, что у уравнения $x^2 + 1 = 0$ есть множество решений (впрочем, пустое), что множество решений системы уравнений есть пересечение множеств решений каждого из них (а для «совокупности» уравнений — объединение), что в множестве $\{2, 2, 3\}$ не три элемента, а два, и оно равно множеству $\{2, 3\}$, что $\varnothing$, $\{\varnothing\}$ и $\{\varnothing, \{\varnothing\}\}$ — это три совершенно разных множества и т. д. Но всё равно большинство школьников так и не поняло, почему множество решений уравнения $x^2 = 4$ можно записывать как $\{-2, 2\}$, а множество решений уравнения $x^2 = -4$ нельзя записывать как $\{\varnothing\}$ (а надо писать $\varnothing$). Отметим кстати ещё два расхождения: в школе натуральные числа начинаются с единицы, а в некоторых книжках — с нуля (мы тоже будем называть нуль натуральным числом). Кроме того, иногда вместо $\subset$ пишут $\subseteq$, используя $\subset$ для собственных подмножеств (вместо нашего $\subsetneq$).

Мы предполагаем, что перечисленные выше основные понятия теории множеств более или менее вам знакомы, и будем достаточно свободно ими пользоваться. Вот несколько задач для самоконтроля; надеемся, что большинство из них не представит для вас большого труда.

1. Старейший математик среди шахматистов и старейший шахматист среди математиков — это один или тот же человек или (возможно) разные?

2. Лучший математик среди шахматистов и лучший шахматист среди математиков — это один или тот же человек или (возможно) разные?

3. Каждый десятый математик — шахматист, а каждый шестой шахматист — математик. Кого больше — математиков или шахматистов — и во сколько раз?

4. Существуют ли такие множества A, B и C, что $A \cap B \neq \varnothing$, $A \cap C = \varnothing$ и $(A \cap B) \setminus C = \varnothing$?

5. Какие из равенств (**а**) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$; (**б**) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$; (**в**) $(A \cup B) \setminus C = (A \setminus C) \cup B$; (**г**) $(A \cap B) \setminus C = (A \setminus C) \cap B$; (**д**) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$; (**е**) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ верны для любых множеств A, B, C?

6. Проведите подробное доказательство верных равенств предыдущей задачи, исходя из определений. (Докажем, что множества в левой и правой частях равны. Пусть x — любой элемент левой части равенства. Тогда... Поэтому x входит в правую часть. Обратно, пусть ...) Приведите контрпримеры к неверным равенствам.

7. Докажите, что операция «симметрическая разность» ассоциативна: $A \triangle (B \triangle C) = (A \triangle B) \triangle C$ для любых A, B и C. (Указание: сложение по модулю 2 ассоциативно.)

8. Докажите, что $(A_1 \cap \ldots \cap A_n) \triangle (B_1 \cap \ldots \cap B_n) \subset (A_1 \triangle B_1) \cup \ldots \cup (A_n \triangle B_n)$ для любых множеств $A_1, \ldots, A_n$ и $B_1, \ldots, B_n$.

9. Докажите, что если какое-то равенство (содержащее переменные для множеств и операции $\cap$, $\cup$, $\setminus$) неверно, то можно найти контрпример к нему, в котором множества пусты или состоят из одного элемента.

10. Сколько различных выражений для множеств можно составить из переменных A и B с помощью (многократно используемых) операций пересечения, объединения и разности? (Два выражения считаются одинаковыми, если они равны при любых значениях переменных.) Тот же вопрос для трёх множеств и для n множеств. (Ответ в общем случае: 2^{2^n-1}.)

11. Тот же вопрос, если используются только операции $\cup$ и $\cap$. (Для двух и трёх переменных это число несложно подсчитать, но общей формулы для n переменных не известно. Эту задачу называют также задачей о числе монотонных булевых функций от n аргументов.)

12. Сколько существует подмножеств у n-элементного множества?

13. Пусть множество A содержит n элементов, а его подмножество B содержит k элементов. Сколько существует множеств C, для которых $B \subset C \subset A$?

14. Множество U содержит $2n$ элементов. В нём выделено k подмножеств, причём ни одно из них не является подмножеством другого. Каково может быть максимальное значение числа k? (Указание. Максимум достигается, когда все подмножества имеют по n элементов. В самом деле, представим себе, что мы начинаем с пустого множества и добавляем по одному элементу, пока не получится множество U. В ходе такого процесса может появиться не более одного выделенного множества; с другой стороны, можно подсчитать математическое ожидание числа выделенных

множеств по линейности; вероятность пройти через данное множество $Z \subset$ $\subset U$ минимальна, когда Z содержит n элементов, поскольку все множества данного размера равновероятны.)

1.2. Число элементов

Число элементов в конечном множестве A называют также его *мощностью* и обозначают $|A|$ (а также $\#A$). (Вскоре мы будем говорить о мощностях и для бесконечных множеств.) Следующая формула позволяет найти мощность объединения нескольких множеств, если известны мощности каждого из них, а также мощности всех пересечений.

Теорема 1 (Формула включений и исключений).

$$\begin{aligned}|A \cup B| &= |A| + |B| - |A \cap B|;\\ |A \cup B \cup C| &= |A| + |B| + |C| -\\ &\quad - |A \cap B| - |A \cap C| - |B \cap C| +\\ &\quad + |A \cap B \cap C|;\end{aligned}$$

вообще $|A_1 \cup \ldots \cup A_n|$ равно

$$\sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots$$

$\lhd$ Это утверждение несложно доказать индукцией по n, но мы приведём другое доказательство. Фиксируем произвольное множество U, подмножествами которого являются множества $A_1, \ldots, A_n$.

Характеристической функцией множества $X \subset U$ называют функцию χ_X, которая равна 1 на элементах X и 0 на остальных элементах U. Операции над подмножествами множества U соответствуют операциям с их характеристическими функциями. В частности, пересечению множеств соответствует произведение характеристических функций: $\chi_{A\cap B}(u) = \chi_A(u)\chi_B(u)$. Дополнению (до U) соответствует функция $1 - \chi$, если χ — характеристическая функция исходного множества.

Число элементов множества можно записать как сумму значений его характеристической функции:

$$|X| = \sum_u \chi_X(u).$$

Объединение $A_1 \cup \ldots \cup A_N$ можно записать как дополнение к пересечению дополнений множеств A_i; в терминах характеристических функций имеем

$$\chi_{A_1 \cup \ldots \cup A_n} = 1 - (1 - \chi_{A_1}) \ldots (1 - \chi_{A_n}).$$

Раскрыв скобки в правой части, мы получим

$$\sum_i \chi_{A_i} - \sum_{i<j} \chi_{A_i}\chi_{A_j} + \sum_{i<j<k} \chi_{A_i}\chi_{A_j}\chi_{A_k} - \ldots$$

и просуммировав левую и правую часть по всем элементам U (обе они есть функции на U), получим формулу включений и исключений. ▷

15. Докажите, что $|A_1 \triangle \ldots \triangle A_n|$ равно

$$\sum_i |A_i| - 2\sum_{i<j} |A_i \cap A_j| + 4 \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots$$

(коэффициенты — последовательные степени двойки).

Подсчёт количеств элементов в конечных множествах относят к *комбинаторике*. Некоторые начальные сведения из комбинаторики приведены дальше в качестве задач. Сейчас нас в первую очередь интересует следующий принцип:

> *если между двумя множествами можно установить взаимно однозначное соответствие, то в них одинаковое число элементов.*

(Взаимная однозначность требует, чтобы каждому элементу первого множества соответствовал ровно один элемент второго и наоборот.)

Вот несколько примеров использования этого принципа.

16. На окружности выбраны 1000 белых точек и одна чёрная. Чего больше — треугольников с вершинами в белых точках или четырёхугольников, у которых одна вершина чёрная, а остальные три белые? (Решение: их поровну, поскольку каждому четырёхугольнику соответствует треугольник, образованный тремя его белыми вершинами.)

17. Каких подмножеств больше у 100-элементного множества: мощности 57 или мощности 43? (Указание: $57 + 43 = 100$.)

18. Докажите, что последовательностей длины n, составленных из нулей и единиц, столько же, сколько подмножеств у множества $\{1, 2, \ldots, n\}$. (Указание: каждому подмножеству $X \subset \{1, 2, \ldots, n\}$ соответствует «характеристическая последовательность», на i-м месте которой стоит единица, если и только если $i \in X$.)

19. Докажите, что последовательностей нулей и единиц длины n, в которых число единиц равно k, равно числу k-элементных подмножеств n-элементного множества.

Это число называется *числом сочетаний из n по k* и обозначается C_n^k в русских книжках; в иностранных обычно используется обозначение $\binom{n}{k}$.

20. Докажите, что $C_n^k = C_n^{n-k}$.

21. Докажите, что $C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$.

22. Пусть U — непустое конечное множество. Докажите, что подмножеств множества U, имеющих чётную мощность, столько же, сколько имеющих нечётную мощность. (Указание: фиксируем элемент $u \in U$ и объединим в пары подмножества, отличающиеся только в точке u.)

23. Докажите, что $C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = 0$. (Указание: как это связано с предыдущей задачей?)

24. Докажите формулу *бинома Ньютона*:

$$(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1} b + \ldots + C_n^k a^{n-k} b^k + \ldots + C_n^n b^n.$$

25. Докажите, что способов расстановки скобок (указывающих порядок действий) в неассоциативном произведении из n элементов столько же, сколько способов разбить выпуклый $(n+1)$-угольник на треугольники непересекающимися диагоналями. (Для произведения трёх множителей есть два варианта $(ab)c$ и $a(bc)$; с другой стороны, есть два способа разрезать четырёхугольник на два треугольника, проведя диагональ. Для произведения четырёх сомножителей и для пятиугольника имеется по 5 вариантов.)

1.3. Равномощные множества

Два множества называют *равномощными*, если между ними можно установить взаимно однозначное соответствие, при котором каждому элементу одного множества соответствует ровно один элемент другого.

Для конечных множеств это означает, что в них одинаковое число элементов, но определение имеет смысл и для бесконечных множеств. Например, отрезки $[0,1]$ и $[0,2]$ равномощны, поскольку отображение $x \mapsto 2x$ осуществляет искомое соответствие.

26. Докажите, что любые два интервала (a,b) и (c,d) на прямой равномощны.

27. Докажите, что любые две окружности на плоскости равномощны. Докажите, что любые два круга на плоскости равномощны.

28. Докажите, что полуинтервал $[0,1)$ равномощен полуинтервалу $(0,1]$.

Несколько более сложна такая задача: доказать, что интервал $(0,1)$ и луч $(0,+\infty)$ равномощны. Это делается так. Заметим, что отображение $x \mapsto 1/x$ является взаимно однозначным соответствием между $(0,1)$ и $(1,+\infty)$, а $x \mapsto (x-1)$ — взаимно однозначным соответствием между $(1,+\infty)$ и $(0,+\infty)$, поэтому их композиция $x \mapsto (1/x)-1$ является искомым взаимно однозначным соответствием между $(0,1)$ и $(0,+\infty)$.

Вообще, как говорят, отношение равномощности есть *отношение эквивалентности*. Это означает, что оно *рефлексивно* (каждое множество равномощно самому себе), *симметрично* (если A равномощно B, то и B равномощно A) и *транзитивно* (если A равномощно B и B равномощно C, то A равномощно C). Свойством транзитивности мы только что воспользовались, взяв луч $(1,+\infty)$ в качестве промежуточного множества.

Ещё несколько примеров:

- Множество бесконечных последовательностей нулей и единиц равномощно множеству всех подмножеств натурального ряда. (В самом деле, сопоставим с каждой последовательностью множество номеров мест, на которых стоят единицы: например, последовательность из одних нулей соответствует пустому множеству, из одних единиц — натуральному ряду, а последовательность $10101010\ldots$ — множеству чётных чисел.)

- Множество бесконечных последовательностей цифр $0,1,2,3$ равномощно множеству бесконечных последовательностей нулей и единиц. (В самом деле, можно закодировать цифры 0, 1, 2, 3 группами 00, 01, 10, 11. Обратное преобразование разбивает последовательность нулей и единиц на пары, после чего каждая пара заменяется на цифру от 0 до 3.)

- Множество бесконечных последовательностей цифр 0, 1, 2 равномощно множеству бесконечных последовательностей цифр 0 и 1. (Можно было бы пытаться рассуждать так: это множество заключено между двумя множествами одной и той же мощности, и потому равномощно каждому из них. Этот ход мыслей правилен, как показывает теорема Кантора–Бернштейна из раздела 1.5. Но здесь можно обойтись и без этой теоремы,

если закодировать цифры 0, 1 и 2 последовательностями 0, 10 и 11: легко сообразить, что всякая последовательность нулей и единиц однозначно разбивается на такие блоки слева направо. Такой способ кодирования называют «префиксным кодом».)

- Пример с последовательностями нулей и единиц можно обобщить: множество подмножеств любого множества U (оно обычно обозначается $P(U)$ и по-английски называется power set) равномощно множеству всех функций, которые ставят в соответствие каждому элементу $x \in U$ одно из чисел 0 и 1 (множество таких функций обычно обозначают 2^U). (В самом деле, каждому множеству $X \subset U$ соответствует его характеристическая функция.)

Мы продолжим этот список, но сначала докажем несколько простых фактов о счётных множествах (равномощных множеству натуральных чисел).

1.4. Счётные множества

Множество называется *счётным*, если оно равномощно множеству $\mathbb{N}$ натуральных чисел, то есть если его можно представить в виде $\{x_0, x_1, x_2, \dots\}$ (здесь x_i — элемент, соответствующий числу i; соответствие взаимно однозначно, так что все x_i различны).

Например, множество целых чисел $\mathbb{Z}$ счётно, так как целые числа можно расположить в последовательность $0, 1, -1, 2, -2, 3, -3, \dots$

Теорема 2. (а) Подмножество счётного множества конечно или счётно.

(б) Всякое бесконечное множество содержит счётное подмножество.

(в) Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно.

$\lhd$ (а) Пусть B — подмножество счётного множества A. Представим множество A как $\{a_0, a_1, a_2, \dots\}$. Выбросим из последовательности $a_0, a_1, \dots$ те члены, которые не принадлежат B (сохраняя порядок оставшихся). Тогда оставшиеся члены образуют либо конечную последовательность (и тогда B конечно), либо бесконечную (и тогда B счётно).

(б) Пусть A бесконечно. Тогда оно непусто и содержит некоторый элемент b_0. Будучи бесконечным, множество A не исчерпывается элементом b_0 — возьмём какой-нибудь другой элемент b_1, и т. д.

Получится последовательность $b_0, b_1, \ldots$; построение не прервётся ни на каком шаге, поскольку A бесконечно. Теперь множество $B = \{b_0, b_1, \ldots\}$ и будет искомым счётным подмножеством. (Заметим, что B вовсе не обязано совпадать с A, даже если A счётно.)

(в) Пусть имеется счётное число счётных множеств $A_1, A_2, \ldots$ Расположив элементы каждого из них слева направо в последовательность ($A_i = \{a_{i0}, a_{i1}, \ldots\}$) и поместив эти последовательности друг под другом, получим таблицу

$$\begin{array}{ccccc} a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\ a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\ a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\ a_{30} & a_{31} & a_{32} & a_{33} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Теперь эту таблицу можно развернуть в последовательность, например, проходя по очереди диагонали:

$$a_{00},\ a_{01}, a_{10},\ a_{02}, a_{11}, a_{20},\ a_{03}, a_{12}, a_{21}, a_{30}, \ldots$$

Если множества A_i не пересекались, то мы получили искомое представление для их объединения. Если пересекались, то из построенной последовательности надо выбросить повторения.

Если множеств конечное число или какие-то из множеств конечны, то в этой конструкции части членов не будет — и останется либо конечное, либо счётное множество. $\triangleright$

29. Описанный проход по диагоналям задаёт взаимно однозначное соответствие между множеством всех пар натуральных чисел (которое обозначается $\mathbb{N} \times \mathbb{N}$) и $\mathbb{N}$. Любопытно, что это соответствие задаётся простой формулой (многочленом второй степени с рациональными коэффициентами). Укажите этот многочлен.

Замечание. В доказательстве утверждения (б) теоремы 2 есть тонкий момент: на каждом шаге мы должны выбрать один из оставшихся элементов множества A; такие элементы есть, но у нас нет никакого правила, позволяющего такой выбор описать. При более формальном построении теории множеств тут нужно сослаться на специальную аксиому, называемую *аксиомой выбора*. Законность этой аксиомы вызывала большие споры в начале 20-го века, но постепенно к ней привыкли, и эти споры сейчас почти не воспринимаются. (К некоторым парадоксальным примерам, связанным с аксиомой выбора, мы ещё вернёмся.) В середине века великий логик Курт Гёдель доказал, что аксиому выбора нельзя опровергнуть, пользуясь

остальными аксиомами теории множеств, а в 1960-е годы американский математик Пол Дж. Коэн доказал, что её нельзя и вывести из остальных аксиом. (Конечно, понимание этих утверждений требует подробного изложения теории множеств как аксиоматической теории.)

30. Такой же тонкий момент (хотя и менее очевидный) есть и в доказательстве утверждения (в). Можете ли вы догадаться, где он? (Ответ: мы знаем, что множества A_i счётны, то есть что для каждого i *существует* взаимно однозначное соответствие между $\mathbb{N}$ и A_i. Но нужно выбрать и фиксировать эти соответствия, прежде чем удастся построить соответствие между объединением всех A_i и $\mathbb{N}$.)

Ещё несколько примеров счётных множеств:

- Множество $\mathbb{Q}$ рациональных чисел счётно. В самом деле, рациональные числа представляются несократимыми дробями с целым числителем и знаменателем. Множество дробей с данным знаменателем счётно, поэтому $\mathbb{Q}$ представимо в виде объединения счётного числа счётных множеств. Забегая вперёд (см. раздел 1.6), отметим, что множество $\mathbb{R}$ всех действительных чисел несчётно.

- Множество $\mathbb{N}^k$, элементами которого являются наборы из k натуральных чисел, счётно. Это легко доказать индукцией по k. При $k = 2$ множество $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ пар натуральных чисел разбивается на счётное число счётных множеств $\{0\} \times \mathbb{N}, \{1\} \times \times \mathbb{N}, \ldots$ (элементами i-го множества будут пары, первый член которых равен i). Поэтому $\mathbb{N}^2$ счётно. Аналогичным образом множество $\mathbb{N}^3$ троек натуральных чисел разбивается на счётное число множеств $\{i\} \times \mathbb{N} \times \mathbb{N}$. Каждое из них состоит из троек, первый член которых фиксирован и потому равномощно множеству $\mathbb{N}^2$, которое счётно. Точно так же можно перейти от счётности множества $\mathbb{N}^k$ к счётности множества $\mathbb{N}^{k+1}$.

  По тем же причинам произведение двух счётных множеств $A \times B$ и вообще конечного числа счётных множеств $A_1 \times \ldots \times A_k$ (элементами этого множества являются наборы $\langle a_1, \ldots, a_k \rangle$, составленные из элементов $a_1 \in A_1, \ldots, a_k \in A_k$) счётно.

- Множество всех конечных последовательностей натуральных чисел счётно. В самом деле, множество всех последовательностей данной длины счётно (как мы только что видели), так

что интересующее нас множество разбивается на счётное число счётных множеств.

- В предыдущем примере не обязательно говорить о натуральных числах — можно взять любое счётное (или конечное) множество. Например, множество всех текстов, использующих русский алфавит (такой текст можно считать конечной последовательностью букв, пробелов, знаков препинания и т. п.), счётно; то же самое можно сказать о множестве (всех мыслимых) компьютерных программ и т. д.

- Число называют *алгебраическим*, если оно является корнем ненулевого многочлена с целыми коэффициентами. Множество алгебраических чисел счётно, так как многочленов счётное число (многочлен задаётся конечной последовательностью целых чисел — его коэффициентов), а каждый многочлен имеет конечное число корней (не более n для многочленов степени n).

- Множество периодических дробей счётно. В самом деле, такая дробь может быть записана как конечная последовательность символов из конечного множества (запятая, цифры, скобки); например, дробь 0,16666... можно записать как 0,1(6). А таких последовательностей счётное множество.

31. Докажите, что любое семейство непересекающихся интервалов на прямой конечно или счётно. (Указание: в каждом интервале найдётся рациональная точка.)

32. (**а**) Докажите, что любое множество непересекающихся восьмёрок на плоскости конечно или счётно. (Восьмёрка — объединение двух касающихся окружностей любых размеров.) (**б**) Сформулируйте и докажите аналогичное утверждение для букв «Т».

33. Докажите, что множество точек строгого локального максимума любой функции действительного аргумента конечно или счётно.

34. Докажите, что множество точек разрыва неубывающей функции действительного аргумента конечно или счётно.

Теорема 3. Если множество A бесконечно, а множество B конечно или счётно, то объединение $A \cup B$ равномощно A.

$\triangleleft$ Можно считать, что B не пересекается с A (пересечение можно выбросить из B, останется по-прежнему конечное или счётное множество).

Выделим в A счётное подмножество P; остаток обозначим через Q. Тогда нам надо доказать, что $B + P + Q$ равномощно $P + Q$

(знак $+$ символизирует объединение непересекающихся множеств). Поскольку $B+P$ и P оба счётны, между ними существует взаимно однозначное соответствие. Его легко продолжить до соответствия между $B+P+Q$ и $P+Q$ (каждый элемент множества Q соответствует сам себе). $\triangleright$

35. Примените эту конструкцию и явно укажите соответствие между отрезком $[0,1]$ и полуинтервалом $[0,1)$.

36. Теорема 3 показывает, что добавление счётного множества к бесконечному не меняет его мощности. Можно ли сказать то же самое про удаление? Докажите, что если A бесконечно и не является счётным, а B конечно или счётно, то $A \setminus B$ равномощно A.

37. Немецкий математик Р. Дедекинд предложил такое определение бесконечного множества: множество бесконечно, если оно равномощно некоторому своему подмножеству, не совпадающему со всем множеством. Покажите, что указанное Дедекиндом свойство действительно определяет бесконечные множества.

Добавляя конечные или счётные множества, легко понять, что прямая, все промежутки на прямой (отрезки, интервалы, полуинтервалы), лучи, их конечные или счётные объединения и т. п. равномощны друг другу.

38. Укажите взаимно однозначное соответствие между множеством $[0,1]\cup[2,3]\cup[4,5]\cup\ldots$ и отрезком $[0,1]$.

39. Докажите, что множество всех прямых на плоскости равномощно множеству всех точек на плоскости. (Указание: и точки, и прямые задаются парами чисел — за небольшими исключениями.)

40. Докажите, что полуплоскость (точки плоскости, лежащие по одну сторону от некоторой прямой) равномощна плоскости. (Это верно независимо от того, включаем мы граничную прямую в полуплоскость или нет.)

Теорема 4. Отрезок $[0,1]$ равномощен множеству всех бесконечных последовательностей нулей и единиц.

$\triangleleft$ В самом деле, каждое число $x \in [0,1]$ записывается в виде бесконечной двоичной дроби. Первый знак этой дроби равен 0 или 1 в зависимости от того, попадает ли число x в левую или правую половину отрезка. Чтобы определить следующий знак, надо выбранную половину поделить снова пополам и посмотреть, куда попадёт x, и т. д.

Это же соответствие можно описать в другую сторону: последовательности $x_0x_1x_2\ldots$ соответствует число, являющееся суммой ряда

$$\frac{x_0}{2}+\frac{x_1}{4}+\frac{x_2}{8}+\ldots$$

(В этом построении мы используем некоторые факты из математического анализа, что не удивительно — нас интересуют свойства действительных чисел.)

Описанное соответствие пока что не совсем взаимно однозначно: двоично-рациональные числа (дроби вида $m/2^n$) имеют два представления. Например, число 3/8 можно записать как в виде 0,011000…, так и в виде 0,010111… Соответствие станет взаимно однозначным, если отбросить дроби с единицей в периоде (кроме дроби 0,1111…, которую надо оставить). Но таких дробей счётное число, поэтому на мощность это не повлияет. ▷

41. Какая двоичная дробь соответствует числу 1/3?

В этом доказательстве можно было бы использовать более привычные десятичные дроби вместо двоичных. Получилось бы, что отрезок $[0,1]$ равномощен множеству всех бесконечных последовательностей цифр $0,1,\ldots,9$. Чтобы перейти отсюда к последовательностям нулей и единиц, можно воспользоваться приёмом, описанным на с. 12.

Теперь всё готово для доказательства удивительного факта:

Теорема 5. Квадрат (со внутренностью) равномощен отрезку.

◁ Квадрат равномощен множеству $[0,1]\times[0,1]$ пар действительных чисел, каждое из которых лежит на отрезке $[0,1]$ (метод координат). Мы уже знаем, что вместо чисел на отрезке можно говорить о последовательностях нулей и единиц. Осталось заметить, что паре последовательностей нулей и единиц $\langle x_0x_1x_2\ldots, y_0y_1y_2\ldots\rangle$ можно поставить в соответствие последовательность-смесь $x_0y_0x_1y_1x_2y_2\ldots$ и что это соответствие будет взаимно однозначным. ▷

Этот результат был получен в 1877 году немецким математиком Георгом Ка́нтором и удивил его самого, поскольку противоречил интуитивному ощущению «размерности» (квадрат двумерен, поэтому вроде бы должен содержать больше точек, чем одномерный отрезок). Вот что Кантор писал Дедекинду (20 июня 1877 года), обсуждая вопрос о равномощности пространств разного числа измерений: «Как мне кажется, на этот вопрос следует ответить утвердительно, хотя на протяжении ряда лет я придерживался противоположного мнения».

В одном из ответных писем Дедекинд отмечает, что результат Кантора не лишает смысла понятие размерности, поскольку можно рассматривать лишь непрерывные в обе стороны соответствия, и тогда пространства разной размерности можно будет различить. Эта гипотеза оказалось верной, хотя не такой простой; первые попытки её доказать, в том числе одна из статей Кантора, содержали ошибки, и только спустя тридцать лет голландский математик Л. Брауэр дал правильное доказательство. Впрочем,

отсутствие непрерывного в обе стороны соответствия между отрезком и квадратом доказать несложно; трудности начинаются в бо́льших размерностях. (Заметим также, что существует непрерывное отображение отрезка в квадрат, которое проходит через любую точку квадрата. Оно называется «кривой Пеано».)

Из теоремы 5 легко получить много других утверждений про равномощность геометрических объектов: круг равномощен окружности, прямая равномощна плоскости и т. п.

Можно также заметить, что пространство (точки которого задаются тремя координатами $\langle x, y, z\rangle$) равномощно плоскости (надо закодировать пару $\langle x, y\rangle$ одним числом), и, следовательно, прямой. То же самое можно проделать и для пространств большей размерности.

42. Докажите, что множество всех конечных последовательностей действительных чисел равномощно $\mathbb{R}$ (множеству всех действительных чисел).

43. Докажите, что множество всех бесконечных последовательностей действительных чисел равномощно $\mathbb{R}$.

Отметим, что мы пока не умеем доказывать, что множество действительных чисел (или множество бесконечных последовательностей нулей и единиц) несчётно. Это будет сделано в разделе 1.6.

Мощность множества действительных чисел называют *мощностью континуума* (от латинского слова, означающего «непрерывный»; имеется в виду, что точка на отрезке может непрерывно двигаться от одного конца к другому).

1.5. Теорема Кантора – Бернштейна

Определение равномощности уточняет интуитивную идею о множествах «одинакового размера». А как формально определить, когда одно множество «больше» другого?

Говорят, что множество A *по мощности не больше* множества B, если оно равномощно некоторому подмножеству множества B (возможно, самому B).

44. Некто предложил такое определение: множество A имеет строго меньшую мощность, чем множество B, если оно равномощно некоторой части множества B, не совпадающей со всем B. Почему это определение неудачно? (Указание. Популярные рассказы о теории множеств часто начинаются с такого парадокса, восходящего к Галилею. Каких чисел больше — всех натуральных чисел или точных квадратов? С одной стороны, точные квадраты составляют лишь небольшую часть натуральных чисел; с другой стороны их можно поставить во взаимно однозначное соответствие со всеми натуральными числами.)

Отношение «иметь не большую мощность» обладает многими естественными свойствами:

- Если A и B равномощны, то A имеет не большую мощность, чем B. (Очевидно.)

- Если A имеет не большую мощность, чем B, а B имеет не большую мощность, чем C, то A имеет не большую мощность, чем C. (Тоже несложно. Пусть A находится во взаимно однозначном соответствии с $B' \subset B$, а B находится во взаимно однозначном соответствии с $C' \subset C$. Тогда при втором соответствии B' соответствует некоторому множеству $C'' \subset C' \subset C$, как показано на рис. 1, и потому A равномощно C''.)

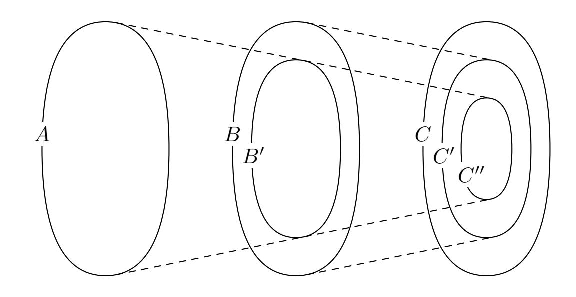


Рис. 1. Транзитивность сравнения мощностей

- Если A имеет не большую мощность, чем B, а B имеет не большую мощность, чем A, то они равномощны. (Это вовсе не очевидное утверждение составляет содержание теоремы Кантора – Бернштейна, которую мы сейчас докажем.)

- Для любых двух множеств A и B верно (хотя бы) одно из двух: либо A имеет не большую мощность, чем B, либо B имеет не большую мощность, чем A. (Доказательство этого факта требует так называемой «трансфинитной индукции»; см. раздел 2.6, теорема 25.)

Теорема 6 (Кантора – Бернштейна). Если множество A равномощно некоторому подмножеству множества B, а B равномощно некоторому подмножеству множества A, то множества A и B равномощны.

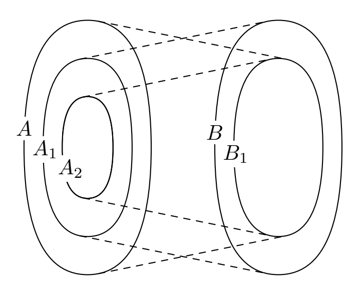


Рис. 2.

◁ Пусть A равномощно подмножеству B_1 множества B, а B равномощно подмножеству A_1 множества A (см. рис. 2). При взаимно однозначном соответствии между B и A_1 подмножество $B_1 \subset B$ переходит в некоторое подмножество $A_2 \subset A_1$. При этом все три множества A, B_1 и A_2 равномощны, — и нужно доказать, что они равномощны множеству B, или, что то же самое, A_1.

Теперь мы можем забыть про множество B и его подмножества и доказывать такой факт:

> *если $A_2 \subset A_1 \subset A_0$ и A_2 равномощно A_0, то все три множества равномощны.*

(Для единообразия мы пишем A_0 вместо A.)

Пусть f — функция, осуществляющая взаимно однозначное соответствие $A_0 \to A_2$ (элемент $x \in A_0$ соответствует элементу $f(x) \in \in A_2$). Когда A_0 переходит в A_2, меньшее множество A_1 переходит в какое-то множество $A_3 \subset A_2$ (см. рис. 3). Аналогичным образом само A_2 переходит в некоторое множество $A_4 \subset A_2$. При этом $A_4 \subset A_3$, так как $A_1 \subset A_2$.

Продолжая эту конструкцию, мы получаем убывающую последовательность множеств

$$A_0 \supset A_1 \supset A_2 \supset A_3 \supset A_4 \supset \ldots$$

и взаимно однозначное соответствие $f\colon A_0 \to A_2$, при котором A_i соответствует A_{i+2} (иногда это записывают так: $f(A_i) = A_{i+2}$). Формально можно описать A_{2n} как множество тех элементов, которые получаются из какого-то элемента множества A_0 после n-кратного применения функции f. Аналогичным образом A_{2n+1} состоит из тех

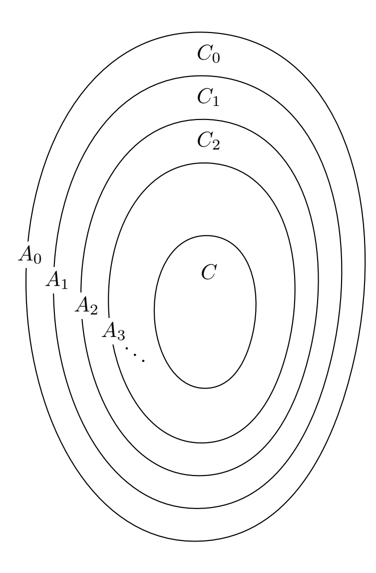


Рис. 3.

и только тех элементов, которые получаются из какого-то элемента множества A_1 после n-кратного применения функции f.

Заметим, что пересечение всех множеств A_i вполне может быть непусто: оно состоит из тех элементов, у которых можно сколько угодно раз брать f-прообраз. Теперь можно сказать так: множество A_0 мы разбили на непересекающиеся слои $C_i = A_i \setminus A_{i+1}$ и на сердцевину $C = \bigcap_i A_i$.

Слои C_0, C_2, C_4, … равномощны (функция f осуществляет взаимно однозначное соответствие между C_0 и C_2, между C_2 и C_4 и т. д.):

$$C_0 \xrightarrow{f} C_2 \xrightarrow{f} C_4 \xrightarrow{f} \ldots$$

То же самое можно сказать про слои с нечётными номерами:

$$C_1 \xrightarrow{f} C_3 \xrightarrow{f} C_5 \xrightarrow{f} \ldots$$

Можно ещё отметить (что, впрочем, не понадобится), что функция f на множестве C осуществляет его перестановку (взаимно однозначное соответствие с самим собой).

Теперь легко понять, как построить взаимно однозначное соответствие g между A_0 и A_1. Пусть $x \in A_0$. Тогда соответствующий

ему элемент $g(x)$ строится так: $g(x) = f(x)$ при $x \in C_{2k}$ и $g(x) = x$ при $x \in C_{2k+1}$ или $x \in C$ (см. рис. 4). ▷

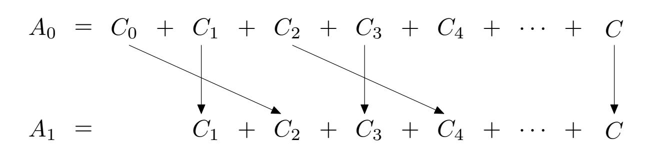


Рис. 4.

История этой теоремы (называемой также теоремой Шрёдера – Бернштейна) такова. Кантор формулирует её без доказательства в 1883 году, обещая: «К этому я ещё вернусь в одной более поздней работе и тогда выявлю своеобразный интерес этой общей теоремы». Однако этого обещания он не выполнил, и первые доказательства были даны Шрёдером (1896) и Бернштейном (1897). Как видно из работ и писем Кантора, он предполагал доказывать эту теорему одновременно с возможностью сравнить любые два множества (см. раздел 2.6, теорема 25), но как именно — остаётся непонятным. (Работы Кантора по теории множеств и его письма переведены на русский язык [4]; все цитаты даются по этому изданию.)

Теорема Кантора – Бернштейна значительно упрощает доказательства равномощности: например, если мы хотим доказать, что бублик и шар в пространстве равномощны, то достаточно заметить, что из бублика можно вырезать маленький шар (гомотетичный большому), а из шара — маленький бублик.

45. Посмотрите на приведённые выше задачи, где требовалось доказать равномощность, и убедитесь, что во многих из них применение теоремы Кантора – Бернштейна сильно упрощает дело.

46. Докажите, что все геометрические фигуры, содержащие хотя бы кусочек прямой или кривой, равномощны.

47. Докажите, что если квадрат разбит на два множества, то хотя бы одно из них равномощно квадрату. (Указание. Если одна из частей содержит отрезок, то можно воспользоваться теоремой Кантора – Бернштейна. Если же, скажем, первая часть не содержит отрезков, то в каждом горизонтальном сечении квадрата есть точка второй части, и с помощью аксиомы выбора во второй части можно найти подмножество, равномощное отрезку — после чего снова можно сослаться на теорему Кантора – Бернштейна.)

48. Докажите, что если отрезок разбит на две части, то хотя бы одна из них равномощна отрезку.

То же самое доказательство теоремы Кантора – Бернштейна мож-

но изложить более абстрактно (и избавиться от упоминания натуральных чисел). Напомним, что $f\colon A \to A_2$ есть взаимно однозначное соответствие между множеством A и его подмножеством A_2, а A_1 — некоторое промежуточное множество. Назовём множество $X \subset \subset A$ «хорошим», если оно содержит $A \setminus A_1$ и замкнуто относительно f, т. е.

$$X \supset (A \setminus A_1) + f(X)$$

(мы используем знак + для объединения, поскольку объединяемые множества заведомо не пересекаются). Легко проверить, что пересечение любого семейства хороших множеств хорошее, поэтому если мы пересечём все хорошие множества, то получим минимальное по включению хорошее множество. Назовём его M. Легко проверить, что множество $(A \setminus A_1) + f(M)$ будет хорошим, поэтому в силу минимальности M включение в определении хорошего множества превращается в равенство:

$$M = (A \setminus A_1) + f(M).$$

Теперь всё готово для построения биекции $g\colon A \to A_1$. Эта биекция совпадает с f внутри M и тождественна вне M.

49. Проведите это рассуждение подробно.

Это рассуждение удобно при построении аксиоматической теории множеств, так как в нём не нужны натуральные числа (которые строятся далеко не сразу). Но по существу это то же самое рассуждение, поскольку M есть $C_0 \cup C_2 \cup \ldots$

50. Пусть f — взаимно однозначное соответствие между A и некоторым подмножеством множества B, а g — взаимно однозначное соответствие между B и некоторым подмножеством множества A. Докажите, что можно так разбить множество A на непересекающиеся части A' и A'', а множество B — на непересекающиеся части B' и B'', что f осуществляет взаимно однозначное соответствие между A' и B', а g — между A'' и B''. (Указание: именно это мы фактически установили при доказательстве теоремы Кантора – Бернштейна.)

51. Докажите, что квадрат можно разбить на две части так, что из подобных им частей можно сложить круг. Формально: квадрат можно разбить на две части A' и A'', а круг — на две части B' и B'', для которых A' подобно B', а A'' подобно B''. (Указание: воспользуйтесь предыдущей задачей.)

Теперь, имея в виду теорему Кантора – Бернштейна, вернёмся к вопросу о сравнении мощностей. Для данных множеств A и B теоретически имеются четыре возможности:

- A равномощно некоторой части B, а B равномощно некоторой части A. (В этом случае, как мы знаем, множества равномощны.)

- A равномощно некоторой части B, но B не равномощно никакой части A. В этом случае говорят, что A *имеет меньшую мощность, чем* B.

- B равномощно некоторой части A, но A не равномощно никакой части B. В этом случае говорят, что A *имеет большую мощность, чем* B.

- Ни A не равномощно никакой части B, ни B не равномощно никакой части A. Этот случай на самом деле невозможен, но мы этого пока не знаем (см. раздел 2.6).

52. Докажите, что счётное множество имеет меньшую мощность, чем любое несчётное.

53. Проверьте аккуратно, что если A имеет меньшую мощность, чем B, а B имеет меньшую мощность, чем C, то A имеет меньшую мощность, чем C (транзитивность сравнения мощностей).

Заметим, что мы уже долго говорим о сравнении мощностей, но воздерживаемся от упоминания «мощности множества» как самостоятельного объекта, а только сравниваем мощности разных множеств. В принципе можно было бы определить мощность множества A как класс всех множеств, равномощных A. Такие классы для множеств A и B совпадают в том и только том случае, когда A и B равномощны, так что слова «имеют равную мощность» приобрели бы буквальный смысл. Проблема тут в том, что таких множеств (равномощных множеству A) слишком много, поскольку всё на свете может быть их элементами. Их насколько много, что образовать из них множество затруднительно, это может привести к парадоксам (см. раздел 1.6, с. 29).

Из этой ситуации есть несколько выходов. Самый простой — по-прежнему говорить только о сравнении мощностей, но не о самих мощностях. Можно также ввести понятие «класса» — такой большой совокупности объектов, что её уже нельзя считать элементом других совокупностей («если вы понимаете, о чём я тут толкую» — добавила бы Сова из книжки о Винни-Пухе), и считать мощностью множества A класс всех множеств, равномощных A. Ещё один выход — для каждого A выбрать некоторое «стандартное» множество,

равномощное A, и назвать его мощностью множества A. Обычно в качестве стандартного множества берут минимальный ординал, равномощный A, — но это построение уже требует более формального (аксиоматического) построения теории множеств.

Кантор говорил о мощностях так (1895): «*Мощностью* или *кардинальным числом* множества M мы называем то общее понятие, которое получается при помощи нашей активной мыслительной способности из M, когда мы абстрагируемся от качества его различных элементов m и от порядка их задания. $\langle \ldots \rangle$ Так как из каждого отдельного элемента m, когда мы отвлекаемся от качества, получается некая „единица", то само кардинальное число оказывается множеством, образованным исключительно из единиц, которое существует как интеллектуальный образ или как проекция заданного множества M в наш разум».

Так или иначе, мы будем употреблять обозначение $|A|$ для мощности множества A хотя бы как вольность речи: $|A| = |B|$ означает, что множества A и B равномощны; $|A| \leqslant |B|$ означает, что A равномощно некоторому подмножеству множества B, а $|A| < |B|$ означает, что A имеет меньшую мощность, чем B (см. с. 24).

1.6. Теорема Кантора

Классический пример неравномощных бесконечных множеств (до сих пор такого примера у нас не было!) даёт «диагональная конструкция Кантора».

Теорема 7 (Кантора). Множество бесконечных последовательностей нулей и единиц несчётно.

$\lhd$ Предположим, что оно счётно. Тогда все последовательности нулей и единиц можно перенумеровать: $\alpha_0, \alpha_1, \ldots$ Составим бесконечную вниз таблицу, строками которой будут наши последовательности:

$$\begin{array}{lllll} \alpha_0 & = & \underline{\alpha_{00}} & \alpha_{01} & \alpha_{02} & \ldots \\ \alpha_1 & = & \alpha_{10} & \underline{\alpha_{11}} & \alpha_{12} & \ldots \\ \alpha_2 & = & \alpha_{20} & \alpha_{21} & \underline{\alpha_{22}} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

(через α_{ij} мы обозначаем j-й член i-й последовательности). Теперь рассмотрим последовательность, образованную стоящими на диагонали членами α_{00}, α_{11}, α_{22}, $\ldots$; её i-й член есть α_{ii} и совпадает с i-м членом i-й последовательности. Заменив все члены на противоположные, мы получим последовательность β, у которой

$$\beta_i = 1 - \alpha_{ii},$$

так что последовательность β отличается от любой из последовательностей α_i (в позиции i) и потому отсутствует в таблице. Это противоречит нашему предположению о том, что таблица включает в себя все последовательности. $\triangleright$

Из этой теоремы следует, что множество $\mathbb{R}$ действительных чисел (которое, как мы видели, равномощно множеству последовательностей нулей и единиц) несчётно. В частности, оно не может совпадать со счётным множеством алгебраических чисел и потому существует действительное число, не являющееся алгебраическим (не являющееся корнем никакого ненулевого многочлена с целочисленными коэффициентами). Такие числа называют *трансцендентными*.

К моменту создания Кантором теории множеств уже было известно, что такие числа существуют. Первый пример такого числа построил в 1844 году французский математик Ж. Лиувилль. Он показал, что число, хорошо приближаемое рациональными, не может быть алгебраическим (таково, например, число $\sum(1/10^{n!})$). Доказательство теоремы Лиувилля не очень сложно, но всё-таки требует некоторых оценок погрешности приближения; на его фоне доказательство Кантора, опубликованное им в 1874 году, выглядит чистой воды фокусом. Эта публикация была первой работой по теории множеств; в её первом параграфе доказывается счётность множества алгебраических чисел, а во втором — несчётность множества действительных чисел. (Общее определение равномощности было дано Кантором лишь через три года, одновременно с доказательством равномощности пространств разного числа измерений, о котором мы уже говорили.)

Отметим кстати, что в том же 1874 году французский математик Ш. Эрмит доказал, что основание натуральных логарифмов $e = 2{,}71828\ldots$ трансцендентно, а через восемь лет немецкий математик Ф. Линдеман доказал трансцендентность числа $\pi = 3{,}1415\ldots$ и тем самым невозможность квадратуры круга.

В нескольких следующих задачах мы предполагаем известными некоторые начальные сведения из курса математического анализа.

54. Покажите, что для всякого несчётного множества $A \subset \mathbb{R}$ можно указать точку a, любая окрестность которой пересекается с A по несчётному множеству. (Утверждение остаётся верным, если слова «несчётное множество» заменить на «множество мощности континуума».)

55. Покажите, что любое непустое замкнутое множество $A \subset \mathbb{R}$ без изолированных точек имеет мощность континуума.

56. Покажите, что любое замкнутое множество $A \subset \mathbb{R}$ либо конечно, либо счётно, либо имеет мощность континуума. (Указание. Рассмотрим множество $B \subset A$, состоящее из тех точек множества A, в любой окрестности которых несчётно много других точек из A. Если B пусто, то A

конечно или счётно. Если B непусто, то оно замкнуто и не имеет изолированных точек.)

Эта задача показывает, что для замкнутых подмножество прямой верна гипотеза континуума, утверждающая, что любое подмножество прямой либо конечно, либо счётно, либо равномощно $\mathbb{R}$. (Кантор, доказавший этот факт, рассматривал его как первый шаг к доказательству гипотезы континуума для общего случая, но из этого ничего не вышло.)

57. Из плоскости выбросили произвольное счётное множество точек. Докажите, что оставшаяся часть плоскости линейно связна и, более того, любые две невыброшенные точки можно соединить двухзвенной ломаной, не задевающей выброшенных точек.

Вернёмся к диагональной конструкции. Мы знаем, что множество последовательностей нулей и единиц равномощно множеству подмножеств натурального ряда (каждому подмножеству соответствует его «характеристическая последовательность», у которой единицы стоят на местах из этого подмножества). Поэтому можно переформулировать эту теорему так:

|| *Множество $\mathbb{N}$ не равномощно множеству своих подмножеств.*

Доказательство также можно шаг за шагом перевести на такой язык: пусть они равномощны; тогда есть взаимно однозначное соответствие $i \mapsto A_i$ между натуральными числами и подмножествами натурального ряда. Диагональная последовательность в этих терминах представляет собой множество тех i, для которых $i \in A_i$, а последовательность β, отсутствовавшая в перечислении, теперь будет его дополнением ($B = \{i \mid i \notin A_i\}$).

При этом оказывается несущественным, что мы имеем дело с натуральным рядом, и мы приходим к такому утверждению:

Теорема 8 (общая формулировка теоремы Кантора). Никакое множество X не равномощно множеству всех своих подмножеств.

$\lhd$ Пусть φ — взаимно однозначное соответствие между X и множеством $P(X)$ всех подмножеств множества X. Рассмотрим те элементы $x \in X$, которые не принадлежат соответствующему им подмножеству. Пусть Z — образованное ими множество:

$$Z = \{x \in X \mid x \notin \varphi(x)\}.$$

Докажем, что подмножество Z не соответствует никакому элементу множества X. Пусть это не так и $Z = \varphi(z)$ для некоторого элемен-

та $z \in X$. Тогда

$$z \in Z \Leftrightarrow z \notin \varphi(z) \Leftrightarrow z \notin Z$$

(первое — по построению множества Z, второе — по предположению $\varphi(z) = Z$). Полученное противоречие показывает, что Z действительно ничему не соответствует, так что φ не взаимно однозначно. $\triangleright$

С другой, стороны, любое множество X равномощно некоторой части множества $P(X)$. В самом деле, каждому элементу $x \in X$ можно поставить в соответствие одноэлементное подмножество $\{x\}$. Поэтому, вспоминая определение сравнения множеств по мощности (с. 24), можно сказать, что мощность множества X всегда меньше мощности множества $P(X)$

58. Докажите, что $n < 2^n$ для всех натуральных $n = 0, 1, 2, \ldots$

В общей формулировке теорема 8 появляется в работе Кантора 1890/91 года. Вместо подмножеств Кантор говорит о функциях, принимающих значения 0 и 1.

На самом деле мы уже приблизились к опасной границе, когда наглядные представления о множествах приводят к противоречию. В самом деле, рассмотрим множество всех множеств U, элементами которого являются все множества. Тогда, в частности, все подмножества множества U будут его элементами, и $P(U) \subset U$, что невозможно по теореме Кантора.

Это рассуждение можно развернуть, вспомнив доказательство теоремы Кантора — получится так называемый парадокс Рассела. Вот как его обычно излагают.

Типичные множества не являются своими элементами. Скажем, множество натуральных чисел $\mathbb{N}$ само не является натуральным числом и потому не будет своим элементом. Однако в принципе можно себе представить и множество, которое является своим элементом (например, множество всех множеств). Назовём такие множества «необычными». Рассмотрим теперь множество всех обычных множеств. Будет ли оно обычным? Если оно обычное, то оно является своим элементом и потому необычное, и наоборот. Как же так?

Модифицированная версия этого парадокса такова: будем называть прилагательное самоприменимым, если оно обладает описываемым свойством. Например, прилагательное «русский» самоприменимо, а прилагательное «глиняный» нет. Другой пример: прилагательное «трёхсложный» самоприменимо, а «двусложный» нет. Теперь вопрос: будет ли прилагательное «несамоприменимый» самоприменимым? (Любой ответ очевидно приводит к противоречию.)

Отсюда недалеко до широко известного «парадокса лжеца», говорящего «я лгу», или до истории о солдате, который должен был брить всех солдат одной с ним части, кто не бреется сам и т. п.

Возвращаясь к теории множеств, мы обязаны дать себе отчёт в том, что плохого было в рассуждениях, приведших к парадоксу Рассела. Вопрос этот далеко не простой, и его обсуждение активно шло всю первую половину 20-го века. Итоги этого обсуждения приблизительно можно сформулировать так:

- Понятие множества не является непосредственно очевидным; разные люди (и научные традиции) могут понимать его по-разному.

- Множества — слишком абстрактные объекты для того, чтобы вопрос «а что на самом деле?» имел смысл. Например, в работе Кантора 1878 года была сформулирована *континуум-гипотеза*: всякое подмножество отрезка либо конечно, либо счётно, либо равномощно всему отрезку. (Другими словами, между счётными множествами и множествами мощности континуум нет промежуточных мощностей). Кантор написал, что это может быть доказано «с помощью некоторого метода индукции, в изложение которого мы не будем входить здесь подробнее», но на самом деле доказать это ему не удалось. Более того, постепенно стало ясно, что утверждение континуум-гипотезы можно считать истинным или ложным, — при этом получаются разные теории множеств, но в общем-то ни одна из этих теорий не лучше другой.

  Тут есть некоторая аналогия с неевклидовой геометрией. Мы можем считать «пятый постулат Евклида» (через данную точку проходит не более одной прямой, параллельной данной) истинным. Тогда получится геометрия, называемая евклидовой. А можно принять в качестве аксиомы противоположное утверждение: через некоторую точку можно провести две различные прямые, параллельные некоторой прямой. Тогда получится неевклидова геометрия. [Отметим, кстати, распространённое заблуждение: почему-то широкие массы писателей о науке и даже отдельные математики в минуты затмений (см. статью в Вестнике Академии Наук, посвящённую юбилею Лобачевского) считают, что в неевклидовой геометрии параллельные прямые пересекаются. Это не так — параллельные прямые и в евкли-

довой, и в неевклидовой геометрии определяются как прямые, которые не пересекаются.]

Вопрос о том, евклидова или неевклидова геометрия правильна «на самом деле», если вообще имеет смысл, не является математическим — скорее об этом следует спрашивать физиков. К теории множеств это относится в ещё большей степени, и разве что теология (Кантор неоднократно обсуждал вопросы теории множеств с профессионалами-теологами) могла бы в принципе претендовать на окончательный ответ.

- Если мы хотим рассуждать о множествах, не впадая в противоречия, нужно проявлять осторожность и избегать определённых видов рассуждений. Безопасные (по крайней мере пока не приведшие к противоречию) правила обращения со множествами сформулированы в аксиоматической теории множеств (формальная теория ZF, названная в честь Цермело и Френкеля). Добавив к этой теории аксиому выбора, получаем теорию, называемую ZFC (choice по-английски — выбор). Есть и другие, менее популярные теории.

Однако формальное построение теории множеств выходит за рамки нашего обсуждения. Поэтому мы ограничимся неформальным описанием ограничений, накладываемых во избежание противоречий: нельзя просто так рассмотреть множество всех множеств или множество всех множеств, не являющихся своими элементами, поскольку класс потенциальных претендентов слишком «необозрим». Множества можно строить лишь постепенно, исходя из уже построенных множеств. Например, можно образовать множество всех подмножеств данного множества (*аксиома степени*). Можно рассмотреть подмножество данного множества, образованное элементами с каким-то свойством (*аксиома выделения*). Можно рассмотреть множество всех элементов, входящих хотя бы в один из элементов данного множества (*аксиома суммы*). Есть и другие аксиомы.

Излагая сведения из теории множеств, мы будем стараться держаться подальше от опасной черты, и указывать на опасность в тех местах, когда возникнет искушение к этой черте приблизиться. Пока что такое место было одно: попытка определить мощность множества как класс (множество) всех равномощных ему множеств.

1.7. Функции

До сих пор мы старались ограничиваться минимумом формальностей и говорили о функциях, их аргументах, значениях, композиции и т. п. без попыток дать определения этих понятий. Сейчас мы дадим формальные определения.

Пусть A и B — два множества. Рассмотрим множество всех упорядоченных пар $\langle a, b\rangle$, где $a \in A$ и $b \in B$. Это множество называется *декартовым произведением* множеств A и B и обозначается $A \times B$. (К вопросу о том, что такое упорядоченная пара, мы ещё вернёмся на с. 36.)

Любое подмножество R множества $A \times B$ называется *отношением* между множествами A и B. Если $A = B$, говорят о *бинарном отношении* на множестве A. Например, на множестве натуральных чисел можно рассмотреть бинарное отношение «быть делителем», обычно обозначаемое символом $|$. Тогда можно в принципе было бы написать $\langle 2, 6\rangle \in |$ и $\langle 2, 7\rangle \notin |$. Обычно, однако, знак отношения пишут между объектами (например, $2|6$).

59. Вопрос для самоконтроля: отношения «быть делителем» и «делиться на» — это одно и то же отношение или разные? (Ответ: конечно, разные — в упорядоченной паре порядок существен.)

Если аргументами функции являются элементы множества A, а значениями — элементы множества B, то можно рассмотреть отношение между A и B, состоящее из пар вида $\langle x, f(x)\rangle$. По аналогии с графиками функций на плоскости такое множество можно назвать графиком функции f. С формальной точки зрения, однако, удобнее не вводить отдельного неопределяемого понятия функции, а вместо этого отождествить функцию с её графиком.

Отношение $F \subset A \times B$ называется *функцией из A в B*, если оно не содержит пар с одинаковым первым членом и разными вторыми. Другими словами, это означает, что для каждого $a \in A$ существует не более одного $b \in B$, при котором $\langle a, b\rangle \in F$.

Те элементы $a \in A$, для которых такое b существует, образуют *область определения* функции F. Она обозначается $\operatorname{Dom} F$ (от английского слова domain). Для любого элемента $a \in \operatorname{Dom} F$ можно определить *значение* функции F на аргументе a («в точке a», как иногда говорят) как тот единственный элемент $b \in B$, для которого $\langle a, b\rangle \in F$. Этот элемент записывают как $F(a)$. Все такие элементы b образуют *множество значений* функции F, которое обозначается $\operatorname{Val} F$.

Если $a \notin \operatorname{Dom} F$, то говорят, что функция *не определена* на a. Заметим, что по нашему определению функция из A в B не обязана быть определена на всех элементах множества A — её область определения может быть любым подмножеством множества A. Симметричным образом множество её значений может не совпадать с множеством B.

Если область определения функции f из A в B совпадает с A, то пишут $f\colon A \to B$.

Пример: *тождественная* функция $\mathrm{id}_A\colon A \to A$ переводит множество A в себя, причём $\mathrm{id}(a) = a$ для любого $a \in A$. Она представляет собой множество пар вида $\langle a, a\rangle$ для всех $a \in A$. (Индекс A в id_A иногда опускают, если ясно, о каком множестве идёт речь.)

Композицией двух функций $f\colon A \to B$ и $g\colon B \to C$ называют функцию $h\colon A \to C$, определённую соотношением $h(x) = g(f(x))$. Другими словами, h представляет собой множество пар

$$\{\langle a, c\rangle \mid \langle a, b\rangle \in f \text{ и } \langle b, c\rangle \in g \text{ для некоторого } b \in B\}.$$

Композиция функций обозначается $g \circ f$ (мы, как и в большинстве книг, пишем справа функцию, которая применяется первой).

Очевидно, композиция (как операция над функциями) ассоциативна, то есть $h \circ (f \circ g) = (h \circ f) \circ g$, поэтому в композиции нескольких подряд идущих функций можно опускать скобки.

Пусть $f\colon A \to B$. *Прообразом* подмножества $B' \subset B$ называется множество всех элементов $x \in A$, для которых $f(x) \in B'$. Оно обозначается $f^{-1}(B')$:

$$f^{-1}(B') = \{x \in A \mid f(x) \in B'\}.$$

Образом множества $A' \subset A$ называется множество всех значений функции f на всех элементах множества A'. Оно обозначается $f(A')$:

$$\begin{aligned} f(A') = \{f(a) \mid a \in A'\} = \\ = \{b \in B \mid \langle a, b\rangle \in f \text{ для некоторого } a \in A'\}. \end{aligned}$$

Строго говоря, обозначение $f(A')$ может привести к путанице (одни и те же круглые скобки употребляются и для значения функции, и для образа множества), но обычно ясно, что имеется в виду.

60. Какие из следующих равенств верны?

$$f(A' \cap A'') = f(A') \cap f(A'');$$
$$f(A' \cup A'') = f(A') \cup f(A'');$$
$$f(A' \setminus A'') = f(A') \setminus f(A'');$$
$$f^{-1}(B' \cap B'') = f^{-1}(B') \cap f^{-1}(B'');$$
$$f^{-1}(B' \cup B'') = f^{-1}(B') \cup f^{-1}(B'');$$
$$f^{-1}(B' \setminus B'') = f^{-1}(B') \setminus f^{-1}(B'');$$
$$f^{-1}(f(A')) \subset A';$$
$$f^{-1}(f(A')) \supset A';$$
$$f(f^{-1}(B')) \subset B';$$
$$f(f^{-1}(B')) \supset B';$$
$$(g \circ f)(A) = g(f(A));$$
$$(g \circ f)^{-1}(C') = f^{-1}(g^{-1}(C'));$$

(Здесь $f\colon A \to B$, $g\colon B \to C$, $A', A'' \subset A$, $B', B'' \subset B$, $C' \subset C$.)

Иногда вместо функций говорят об отображениях (резервируя термин «функция» для отображений с числовыми аргументами и значениями). Мы не будем строго придерживаться таких различий, употребляя слова «отображение» и «функция» как синонимы.

Функция $f\colon A \to B$ называется *инъективной*, или *инъекцией*, или *вложением*, если она переводит разные элементы в разные, то есть если $f(a_1) \neq f(a_2)$ при различных a_1 и a_2.

Функция $f\colon A \to B$ называется *сюръективной*, или *сюръекцией*, или *наложением*, если множество её значений есть всё B. (Иногда такие функции называют *отображениями на* B.)

Эти два определения более симметричны, чем может показаться на первый взгляд, как показывают такие задачи:

61. Докажите, что функция $f\colon A \to B$ является вложением тогда и только тогда, когда она имеет *левую обратную* функцию $g\colon B \to A$, то есть функцию g, для которой $g \circ f = \mathrm{id}_A$. Докажите, что функция $f\colon A \to B$ является наложением тогда и только тогда, когда она имеет *правую обратную* функцию $g\colon B \to A$, для которой $f \circ g = \mathrm{id}_B$.

62. Докажите, что функция $f\colon A \to B$ является вложением тогда и только тогда, когда на неё можно сокращать слева: из равенства $f \circ g_1 = f \circ g_2$ следует равенство $g_1 = g_2$ (для любых функций g_1, g_2, области значений которых содержатся в A). Докажите, что функция $f\colon A \to B$ является наложением тогда и только тогда, когда на неё можно сокращать

справа: из равенства $g_1 \circ f = g_2 \circ f$ следует равенство $g_1 = g_2$ (для любых функций g_1, g_2, область определения которых есть B).

Отображение (функция) $f\colon A \to B$, которое одновременно является инъекцией и сюръекцией (вложением и наложением), называется *биекцией*, или взаимно однозначным соответствием.

Если f — биекция, то существует *обратная* функция f^{-1}, для которой $f^{-1}(y) = x \Leftrightarrow f(x) = y$.

63. Могут ли для некоторой функции левая и правая обратные существовать, но быть различны?

Напомним, что множества A и B равномощны, если существует биекция $f\colon A \to B$. В каком случае существует инъекция (вложение) $f\colon A \to B$? Легко понять, что вложение является взаимно однозначным соответствием между A и некоторым подмножеством множества B, поэтому такое вложение существует тогда и только тогда, когда в B есть подмножество, равномощное A, т. е. когда мощность A не превосходит мощности B (в смысле определения, данного в разделе 1.5).

Чуть менее очевиден другой результат: наложение A на B существует тогда и только тогда, когда мощность B не превосходит мощности A.

В самом деле, пусть наложение $f\colon A \to B$ существует. Для каждого элемента $b \in B$ найдётся хотя бы один элемент $a \in A$, для которого $f(a) = b$. Выбрав по одному такому элементу, мы получим подмножество $A' \subset A$, которое находится во взаимно однозначном соответствии с множеством B. (Здесь снова используется аксиома выбора, о которой мы говорили на с. 14.)

В обратную сторону: если какое-то подмножество A' множества A равномощно множеству B и имеется биекция $g\colon A' \to B$, то наложение A на B можно получить, доопределив эту биекцию на элементах вне A' каким угодно образом.

64. Найдите ошибку в этом рассуждении, не читая дальше.

На самом деле такое продолжение возможно, только если B непусто, так что правильное утверждение звучит так: наложение A на B существует только и только тогда, когда B непусто и равномощно некоторому подмножеству A, или когда оба множества пусты.

В нашем изложении остаётся ещё один не вполне понятный момент: что такое «упорядоченная пара»? Неформально говоря, это способ из двух объектов x и y образовать один объект $\langle x, y\rangle$, причём

этот способ обладает таким свойством:

$$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \ \Leftrightarrow\ x_1 = x_2 \text{ и } y_1 = y_2.$$

В принципе, можно так и считать понятие упорядоченной пары неопределяемым, а это свойство — аксиомой. Однако при формальном построении теории множеств удобно использовать трюк, придуманный польским математиком Куратовским, и избежать появления отдельного понятия упорядоченной пары. Прежде чем описывать этот трюк, напомним, что $\{x\}$ обозначает множество, единственным элементом которого является x, а $\{x, y\}$ обозначает множество, которое содержит x и y и не содержит других элементов. Тем самым $\{x, y\} = \{x\} = \{y\}$, если $x = y$.

Теорема 9 (Упорядоченная пара по Куратовскому). Определим $\langle x, y\rangle$ как $\{\{x\}, \{x, y\}\}$. Тогда выполнено указанное выше свойство:

$$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \ \Leftrightarrow\ x_1 = x_2 \text{ и } y_1 = y_2.$$

$\lhd$ В одну сторону это очевидно: если $x_1 = x_2$ и $y_1 = y_2$, то $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$. В другую сторону: пусть $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$. По определению это означает, что

$$\{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\}.$$

Теперь нужно аккуратно разобрать случаи (не путая при этом x с $\{x\}$). Это удобно делать в следующем порядке. Пусть сначала $x_1 \neq y_1$. Тогда множество $\{x_1, y_1\}$ состоит из двух элементов. Раз оно принадлежит левой части равенства, то принадлежит и правой. Значит, оно равно либо $\{x_2\}$, либо $\{x_2, y_2\}$. Первое невозможно, так как двухэлементное множество не может быть равно одноэлементному. Значит, $\{x_1, y_1\} = \{x_2, y_2\}$. С другой стороны, одноэлементное множество $\{x_1\}$ принадлежит левой части равенства, поэтому оно принадлежит и правой, и потому равно $\{x_2\}$ (поскольку не может быть равно двухэлементному). Отсюда $x_1 = x_2$ и $y_1 = y_2$, что и требовалось.

Аналогично разбирается симметричный случай, когда $x_2 \neq y_2$.

Осталось рассмотреть ситуацию, когда $x_1 = y_1$ и $x_2 = y_2$. В этом случае $\{x_1, y_1\} = \{x_1\}$ и потому левая часть данного нам равенства есть $\{\{x_1\}\}$. Аналогичным образом, правая его часть есть $\{\{x_2\}\}$, и потому $x_1 = x_2$, так что все четыре элемента x_1, x_2, y_1, y_2 совпадают. $\rhd$

Заметим, что возможны и другие определения упорядоченной пары, для которых аналогичное утверждение верно, так что никакого «философского смысла» в этом определении нет — это просто удобный технический приём.

65. Докажите утверждение теоремы 9 для *упорядоченной пары по Винеру*: $\langle x, y\rangle = \{\{\varnothing, \{x\}\}, \{\{y\}\}\}$.

1.8. Операции над мощностями

Мощности конечных множеств — натуральные числа, и их можно складывать, умножать, возводить в степень. Эти операции можно обобщить и на мощности бесконечных множеств, и делается это так.

Пусть A и B — два множества. Чтобы сложить их мощности, надо взять мощность множества $A \cup B$, если A и B не пересекаются. Если они пересекаются, то их надо заменить на непересекающиеся равномощные им множества A' и B'. Мощность объединения и будет *суммой* мощностей множеств A и B.

Замечания. 1. Чтобы избежать упоминания мощностей как самостоятельных объектов, следует считать выражение «мощность множества C есть сумма мощностей множеств A и B» идиоматическим выражением (а сказанное выше — его определением). Но мы для удобства будем часто пренебрегать такими предосторожностями.

2. В принципе следовало бы проверить корректность этого определения и доказать, что мощность множества $A' \cup B'$ не зависит от того, какие именно непересекающиеся множества A' и B' (равномощные A и B) мы выберем. (Что, впрочем, очевидно.)

3. Для конечных множеств получается обычное сложение натуральных чисел.

4. Наконец, формально следовало бы ещё доказать, что такие A' и B' можно выбрать. Это можно сделать, например, так: положим $A' = A \times \{0\}$ и $B' = B \times \{1\}$.

Последней проблемы не будет при определении *произведения* мощностей как мощности декартова произведения $A \times B$. (Но остальные замечания остаются в силе.)

Теперь определим *возведение в степень*. Для этого рассмотрим (для данных A и B) множество всех функций вида $f\colon B \to A$ (напомним: это означает, что их область определения есть B, а область значений содержится в A). Это множество обозначается A^B, и его мощность и будет результатом операции возведения в степень.

Если множества A и B конечны и содержат a и b элементов соответственно, то A^B содержит как раз a^b элементов. В самом деле,

определяя функцию $f\colon B \to A$, мы должны определить её значение на каждом из b элементов. Это можно сделать a способами, так что получаем всего a^b вариантов.

66. Чему равно 0^0 согласно нашему определению? (Ответ: единице.)

Пример. Обозначим через 2 какое-нибудь множество из двух элементов, например, $\{0, 1\}$. Что такое $2^{\mathbb{N}}$? По определению это множество функций $f\colon \mathbb{N} \to \{0, 1\}$. Такие функции — это по существу последовательности нулей и единиц, только вместо $f_0 f_1 f_2 \ldots$ мы пишем $f(0), f(1), f(2), \ldots$ (Формально последовательность элементов некоторого множества X так и определяется — как функция типа $\mathbb{N} \to X$.)

Заметим, что 2^X равномощно $P(X)$ (в частном случае $X = \mathbb{N}$ мы это доказывали; для общего случая доказательство такое же).

Обычные свойства сложения и умножения (коммутативность, ассоциативность и дистрибутивность) сохраняют силу и для арифметики мощностей:

$$\begin{aligned}
a + b &= b + a;\\
a + (b + c) &= (a + b) + c;\\
a \times b &= b \times a;\\
a \times (b \times c) &= (a \times b) \times c;\\
(a + b) \times c &= (a \times c) + (b \times c).
\end{aligned}$$

Формально их следует читать, избегая слова «мощность» как самостоятельного объекта: например, $a \times b = b \times a$ означает, что $A \times B$ и $B \times A$ равномощны (и это легко проверить: $\langle x, y\rangle \mapsto \langle y, x\rangle$ будет взаимно однозначным соответствием между ними). Остальные свойства доказываются столь же просто. Чуть сложнее свойства, включающие возведение в степень:

$$\begin{aligned}
a^{b+c} &= a^b \times a^c;\\
(ab)^c &= a^c \times b^c;\\
(a^b)^c &= a^{b\times c}.
\end{aligned}$$

Проверим первое из них. Из чего состоит A^{B+C}? (Будем считать, что B и C не пересекаются.) Его элементами являются функции со значениями в A, определённые на $B + C$. Такая функция состоит из двух частей: своего сужения на B (значения на аргументах из B остаются теми же, остальные отбрасываются) и своего сужения на C.

Тем самым для каждого элемента множества A^{B+C} мы получаем пару элементов из A^B и A^C. Это и будет искомое взаимно однозначное соответствие.

С соответствием между множествами $(A{\times}B)^C$ и $A^C{\times}B^C$ мы тоже часто сталкиваемся. Например, элемент множества $(\mathbb{R}\times\mathbb{R})^{\mathbb{R}}$ есть отображение типа $\mathbb{R}\to\mathbb{R}\times\mathbb{R}$, то есть кривая $t\mapsto z(t)=\langle x(t),y(t)\rangle$ на плоскости. Такая кривая задаётся парой функций $x,y\colon\mathbb{R}\to\mathbb{R}$.

Соответствие между $(A^B)^C$ и $A^{(B\times C)}$ встречается несколько реже. Элемент $f\in A^{(B\times C)}$ является отображением $B\times C\to A$, то есть, в обычной терминологии, функцией двух аргументов (первый из B, второй из C). Если зафиксировать в ней второй аргумент, то получится функция $f_c\colon B\to A$, определённая соотношением $f_c(b)= f(b,c)$ (точнее, $f(\langle b,c\rangle)$). Отображение $c\mapsto f_c$, принадлежащее $(A^B)^C$, и соответствует элементу $f\in A^{(B\times C)}$. (Отчасти сходная конструкция встречается в алгебре, когда многочлен от двух переменных рассматривают как многочлен от одной переменной с коэффициентами в кольце многочленов от второй переменной.)

Мощность счётного множества символически обозначается $\aleph_0$, мощность континуума (отрезка или множества бесконечных последовательностей нулей и единиц) обозначается $\mathfrak{c}$, так что $\mathfrak{c}=2^{\aleph_0}$.

(Естественный вопрос: каков смысл индекса 0 в $\aleph_0$? что такое, скажем, $\aleph_1$? Обычно $\aleph_1$ обозначает наименьшую несчётную мощность (как мы увидим, такая существует). Гипотеза континуума, о которой мы упоминали на с. 30, утверждает, что $\mathfrak{c}=\aleph_1$.)

Известные нам свойства счётных множеств можно записать так:

- $\aleph_0+n=\aleph_0$ для конечного n (объединение счётного и конечного множеств счётно);
- $\aleph_0+\aleph_0=\aleph_0$ (объединение двух счётных множеств счётно);
- $\aleph_0\times\aleph_0=\aleph_0$ (объединение счётного числа счётных множеств счётно).

Отсюда можно формально получить многие факты манипуляциями с мощностями. Например, цепочка равенств

$$\mathfrak{c}\times\mathfrak{c}=2^{\aleph_0}\times 2^{\aleph_0}=2^{\aleph_0+\aleph_0}=2^{\aleph_0}=\mathfrak{c}$$

показывает, что прямая и плоскость равномощны.

Аналогичным образом,

$$\mathfrak{c}^{\aleph_0}=(2^{\aleph_0})^{\aleph_0}=2^{\aleph_0\times\aleph_0}=2^{\aleph_0}=\mathfrak{c}.$$

67. Объясните подробно выкладку:

$$\mathfrak{c}+\mathfrak{c}=1\times\mathfrak{c}+1\times\mathfrak{c}=2\times\mathfrak{c}=2^1\times 2^{\aleph_0}=2^{1+\aleph_0}=2^{\aleph_0}=\mathfrak{c}.$$

68. Проверьте, что $\aleph_0\times\mathfrak{c}=\mathfrak{c}$.

Приведённые нами свойства мощностей полезно сочетать с теоремой Кантора – Бернштейна. Например, заметим, что

$$\mathfrak{c}=2^{\aleph_0}\leqslant {\aleph_0}^{\aleph_0}\leqslant \mathfrak{c}^{\aleph_0}=\mathfrak{c},$$

поэтому ${\aleph_0}^{\aleph_0}=\mathfrak{c}$ (словами: множество всех бесконечных последовательностей натуральных чисел имеет мощность континуума).

69. Последнее рассуждение неявно использует монотонность операции возведения в степень для мощностей (если $a_1\leqslant a_2$, то $a_1^b\leqslant a_2^b$). Проверьте это и аналогичные свойства для других операций (впрочем, почти очевидные).

70. Установите явное соответствие между последовательностями натуральных чисел и иррациональными числами на отрезке $(0,1)$, используя цепные дроби, то есть дроби вида $1/(n_0+1/(n_1+1/(n_2+\ldots)))$.

71. Проверьте, что $\mathfrak{c}^{\mathfrak{c}}=\aleph_0^{\mathfrak{c}}=2^{\mathfrak{c}}$. (Напомним, что по теореме Кантора эта мощность больше мощности континуума.)

72. Какова мощность множества всех непрерывных функций с действительными аргументами и значениями? Существенна ли здесь непрерывность?

73. Какова мощность множества всех монотонных функций с действительными аргументами и значениями?

74. Может ли семейство подмножеств натурального ряда быть несчётным, если любые два его элемента имеют конечное пересечение? конечную симметрическую разность?

Впоследствии мы увидим, что для бесконечных мощностей действуют простые правила $a\times b=a+b=\max(a,b)$, но пока этого мы доказать не можем. Поэтому в задачах 47, 48 нам пришлось воспользоваться обходным манёвром, чтобы доказать, что из $a+b=\mathfrak{c}$ следует $a=\mathfrak{c}$ или $b=\mathfrak{c}$. Следующее утверждение обобщает этот приём:

Теорема 10. Если множество $A_1\times A_2\times\ldots\times A_n$ разбито на непересекающиеся части $B_1,\ldots,B_n$, то найдётся такое i, при котором мощность B_i не меньше мощности A_i.

$\triangleleft$ В самом деле, рассмотрим проекцию множества $B_i\subset A_1\times\ldots\times A_n$ на A_i. Если хотя бы при одном i она покрывает A_i полностью,

то всё доказано. Если нет, выберем для каждого i непокрытую точку x_i. Набор $\langle x_1, \ldots, x_n \rangle$ не входит ни в одно из множеств B_i, что противоречит предположению. ▷

Заметим, что в формулировке этого утверждения (которое иногда называют теоремой Кёнига) говорится о декартовом произведении конечного числа множеств, которое можно определить индуктивно (скажем, $A \times B \times C$ будет состоять из троек $\langle a, b, c \rangle$, которые суть пары $\langle \langle a, b \rangle, c \rangle$). Декартово произведение счётного числа множеств уже так не определишь. Выход такой: $A_0 \times A_1 \times A_2 \times \ldots$ (счётное число сомножителей) можно определить как множество всех последовательностей $a_0, a_1, a_2, \ldots$, у которых $a_i \in A_i$, то есть как множество всех функций a, определённых на $\mathbb{N}$ со значениями в объединении всех A_i, причём $a(i) \in A_i$ при всех i. После такого определения теорема 10 легко переносится и на счётные (а также и на любые) произведения.

Переходя к отрицаниям, теорему Кёнига можно сформулировать так: если при всех $i = 0, 1, 2, \ldots$ для мощностей a_i и b_i выполнено неравенство $b_i < a_i$, то

$$b_0 + b_1 + b_2 + \ldots < a_0 \times a_1 \times a_2 \times \ldots$$

Учитывая, что $\mathfrak{c} \times \mathfrak{c} \times \ldots$ (счётное произведение) равно $\mathfrak{c}^{\aleph_0}$, то есть $\mathfrak{c}$, можно сформулировать такое следствие теоремы Кёнига: если континуум разбит на счётное число подмножеств, то одно из них имеет мощность континуума.

75. Докажите подробно это утверждение.

76. Пусть $a_0, a_1, a_2, \ldots$ — мощности, причём $a_i \geqslant 2$ для всех i. Покажите, что

$$a_0 + a_1 + a_2 + \ldots \leqslant a_0 \times a_1 \times a_2 \times \ldots$$

77. Пусть $m_0 < m_1 < m_2 < \ldots$ — возрастающая последовательность мощностей. Докажите, что сумма $m_0 + m_1 + m_2 + \ldots$ не представима в виде $a^{\aleph_0}$ ни для какой мощности a.

2. Упорядоченные множества

2.1. Отношения эквивалентности и порядка

Напомним, что бинарным отношением на множестве X называется подмножество $R \subset X \times X$; вместо $\langle x_1, x_2 \rangle \in R$ часто пишут $x_1 R x_2$.

Бинарное отношение R на множестве X называется *отношением эквивалентности*, если выполнены следующие свойства:

- (рефлексивность) xRx для всех $x \in X$;
- (симметричность) $xRy \Rightarrow yRx$ для всех $x, y \in X$;
- (транзитивность) xRy и $yRz \Rightarrow xRz$ для всех $x, y, z \in X$.

Имеет место следующее очевидное, но важное утверждение:

Теорема 11. (а) Если множество X разбито в объединение непересекающихся подмножеств, то отношение «лежать в одном подмножестве» является отношением эквивалентности.

(б) Всякое отношение эквивалентности получается описанным способом из некоторого разбиения.

$\triangleleft$ Первое утверждение совсем очевидно; мы приведём доказательство второго, чтобы было видно, где используются все пункты определения эквивалентности. Итак, пусть R — отношение эквивалентности. Для каждого элемента $x \in X$ рассмотрим его *класс эквивалентности* — множество всех $y \in X$, для которых верно xRy.

Докажем, что для двух различных x_1, x_2 такие множества либо не пересекаются, либо совпадают. Пусть они пересекаются, то есть имеют общий элемент z. Тогда $x_1 R z$ и $x_2 R z$, откуда $z R x_2$ (симметричность) и $x_1 R x_2$ (транзитивность), а также $x_2 R x_1$ (симметричность). Поэтому для любого z из $x_1 R z$ следует $x_2 R z$ (транзитивность) и наоборот.

Осталось заметить, что в силу рефлексивности каждый элемент x принадлежит задаваемому им классу, то есть действительно всё множество X разбито на непересекающиеся классы. $\triangleright$

78. Покажите, что требования симметричности и транзитивности можно заменить одним: xRz и $yRz \Rightarrow xRy$ (при сохранении требования рефлексивности).

79. Сколько различных отношений эквивалентности существует на множестве $\{1, 2, 3, 4, 5\}$?

80. На множестве M заданы два отношения эквивалентности, обозначаемые $\sim_1$ и $\sim_2$, имеющие n_1 и n_2 классов эквивалентности соответственно. Будет ли их пересечение $x \sim y \Leftrightarrow [(x \sim_1 y)$ и $(x \sim_2 y)]$ отношением

эквивалентности? Сколько у него может быть классов? Что можно сказать про объединение отношений?

81. (Теорема Рамсея) Множество всех k-элементных подмножеств бесконечного множества A разбито на l классов (k, l — натуральные числа). Докажите, что найдётся бесконечное множество $B \subset A$, все k-элементные подмножества которого принадлежат одному классу.

(При $k = 1$ это очевидно: если бесконечное множество разбито на конечное число классов, то один из классов бесконечен. При $k = 2$ и $l = 2$ утверждение можно сформулировать так: из бесконечного множества людей можно выбрать либо бесконечно много попарно знакомых, либо бесконечно много попарно незнакомых. Конечный вариант этого утверждения — о том, что среди любых шести людей есть либо три попарно знакомых, либо три попарно незнакомых, — известная задача для школьников.)

Множество классов эквивалентности называют *фактор-множеством* множества X по отношению эквивалентности R. (Если отношение согласовано с дополнительными структурами на X, получаются фактор-группы, фактор-кольца и т. д.)

Отношения эквивалентности нам не раз ещё встретятся, но сейчас наша основная тема — отношения порядка.

Бинарное отношение $\leqslant$ на множестве X называется *отношением частичного порядка*, если выполнены такие свойства:

- (рефлексивность) $x \leqslant x$ для всех $x \in X$;
- (антисимметричность) $x \leqslant y$ и $y \leqslant x \Rightarrow x = y$ для всех $x, y \in X$;
- (транзитивность) $x \leqslant y$ и $y \leqslant z \Rightarrow x \leqslant z$ для всех $x, y, z \in X$.

(Следуя традиции, мы используем символ $\leqslant$ (а не букву) как знак отношения порядка.) Множество с заданным на нём отношением частичного порядка называют *частично упорядоченным*.

Говорят, что два элемента x, y частично упорядоченного множества *сравнимы*, если $x \leqslant y$ или $y \leqslant x$. Заметим, что определение частичного порядка не требует, чтобы любые два элемента множества были сравнимы. Добавив это требование, мы получим определение *линейного порядка* (*линейно упорядоченного множества*).

Приведём несколько примеров частичных порядков:

- Числовые множества с обычным отношением порядка (здесь порядок будет линейным).

- На множестве $\mathbb{R} \times \mathbb{R}$ всех пар действительных чисел можно ввести частичный порядок, считая, что $\langle x_1, x_2 \rangle \leqslant \langle y_1, y_2 \rangle$, если $x_1 \leqslant x_2$ и $y_1 \leqslant y_2$. Этот порядок уже не будет линейным: пары $\langle 0, 1 \rangle$ и $\langle 1, 0 \rangle$ не сравнимы.

- На множестве функций с действительными аргументами и значениями можно ввести частичный порядок, считая, что $f \leqslant g$, если $f(x) \leqslant g(x)$ при всех $x \in \mathbb{R}$. Этот порядок не будет линейным.

- На множестве целых положительных чисел можно определить порядок, считая, что $x \leqslant y$, если x делит y. Этот порядок тоже не будет линейным.

- Отношение «любой простой делитель числа x является также и делителем числа y» не будет отношением порядка на множестве целых положительных чисел (оно рефлексивно и транзитивно, но не антисимметрично).

- Пусть U — произвольное множество. Тогда на множестве $P(U)$ всех подмножеств множества U отношение включения $\subset$ будет частичным порядком.

- На буквах русского алфавита традиция определяет некоторый порядок (а $\leqslant$ б $\leqslant$ в $\leqslant \ldots \leqslant$ я). Этот порядок линеен — про любые две буквы можно сказать, какая из них раньше (при необходимости заглянув в словарь).

- На словах русского алфавита определён *лексикографический* порядок (как в словаре). Формально определить его можно так: если слово x является началом слова y, то $x \leqslant y$ (например, кант $\leqslant$ кантор). Если ни одно из слов не является началом другого, посмотрим на первую по порядку букву, в которой слова отличаются: то слово, где эта буква меньше в алфавитном порядке, и будет меньше. Этот порядок также линеен (иначе что бы делали составители словарей?).

- Отношение равенства $((x \leqslant y) \Leftrightarrow (x = y))$ также является отношением частичного порядка, для которого никакие два различных элемента не сравнимы.

- Приведём теперь бытовой пример. Пусть есть множество X картонных коробок. Введём на нём порядок, считая, что $x \leqslant y$,

если коробка x целиком помещается внутрь коробки y (или если x и y — одна и та же коробка). В зависимости от набора коробок этот порядок может быть или не быть линейным.

Пусть x, y — элементы частично упорядоченного множества X. Говорят, что $x < y$, если $x \leqslant y$ и $x \neq y$. Для этого отношения выполнены такие свойства:

$$x \not< x;$$
$$(x < y) \text{ и } (y < z) \;\Rightarrow\; x < z.$$

(Первое очевидно, проверим второе: если $x < y$ и $y < z$, то есть $x \leqslant y$, $x \neq y$, $y \leqslant z$, $y \neq z$, то $x \leqslant z$ по транзитивности; если бы оказалось, что $x = z$, то мы бы имели $x \leqslant y \leqslant x$ и потому $x = y$ по антисимметричности, что противоречит предположению.)

Терминологическое замечание: мы читаем знак $\leqslant$ как «меньше или равно», а знак $<$ — как «меньше», неявно подразумевая, что $x \leqslant y$ тогда и только тогда, когда $x < y$ или $x = y$. К счастью, это действительно так. Ещё одно замечание: выражение $x > y$ («x больше y») означает, что $y < x$, а выражение $x \geqslant y$ («x больше или равно y») означает, что $y \leqslant x$.

82. Объясните, почему не стоит читать $x \leqslant y$ как «x не больше y».

В некоторых книжках отношение частичного порядка определяется как отношение $<$, удовлетворяющее двум указанным свойствам. В этом случае отношение $x \leqslant y \Leftrightarrow [(x < y) \text{ или } (x = y)]$ является отношением частичного порядка в смысле нашего определения.

83. Проверьте это.

Во избежание путаницы отношение $<$ иногда называют отношением *строгого порядка*, а отношение $\leqslant$ — отношением *нестрогого порядка*. Одно и то же частично упорядоченное множество можно задавать по-разному: можно сначала определить отношение нестрогого порядка $\leqslant$ (рефлексивное, антисимметричное и транзитивное) и затем из него получить отношение строгого порядка $<$, а можно действовать и наоборот.

84. Опуская требование антисимметричности в определении частичного порядка, получаем определение *предпорядка*. Докажите, что любой предпорядок устроен так: множество делится на непересекающиеся классы, при этом $x \leqslant y$ для любых двух элементов x, y из одного класса, а на фактор-множестве задан частичный порядок, который и определяет результат сравнения двух элементов из разных классов.

Вот несколько конструкций, позволяющих строить одни упорядоченные множества из других.

- Пусть Y — подмножество частично упорядоченного множества $(X, \leqslant)$. Тогда на множестве Y возникает естественный частичный порядок, *индуцированный* из X. Формально говоря,

$$(\leqslant_Y) = (\leqslant) \cap (Y \times Y).$$

  Если порядок на X был линейным, то и индуцированный порядок на Y, очевидно, будет линейным.

- Пусть X и Y — два непересекающихся частично упорядоченных множества. Тогда на их объединении можно определить частичный порядок так: внутри каждого множества элементы сравниваются как раньше, а любой элемент множества X по определению меньше любого элемента Y. Это множество естественно обозначить $X + Y$. (Порядок будет линейным, если он был таковым на каждом из множеств.)

  Это же обозначение применяют и для пересекающихся (и даже совпадающих множеств). Например, говоря об упорядоченном множестве $\mathbb{N} + \mathbb{N}$, мы берём две непересекающиеся копии натурального ряда $\{0, 1, 2, \ldots\}$ и $\{\bar{0}, \bar{1}, \bar{2}, \ldots\}$ и рассматриваем множество $\{0, 1, 2, \ldots, \bar{0}, \bar{1}, \bar{2}, \ldots\}$, причём $k \leqslant \bar{l}$ при всех k и l, а внутри каждой копии порядок обычный.

- Пусть $(X, \leqslant_X)$ и $(Y, \leqslant_Y)$ — два упорядоченных множества. Можно определить порядок на произведении $X \times Y$ несколькими способами. Можно считать, что $\langle x_1, y_1 \rangle \leqslant \langle x_2, y_2 \rangle$, если $x_1 \leqslant_X x_2$ и $y_1 \leqslant_Y y_2$ (покоординатное сравнение). Этот порядок, однако, не будет линейным, даже если исходные порядки и были линейными: если первая координата больше у одной пары, а вторая у другой, как их сравнить? Чтобы получить линейный порядок, договоримся, какая координата будет «главной» и будем сначала сравнивать по ней, а потом (в случае равенства) — по другой. Если главной считать X-координату, то $\langle x_1, y_1 \rangle \leqslant \langle x_2, y_2 \rangle$, если $x_1 <_X x_2$ или если $x_1 = x_2$, а $y_1 \leqslant_Y y_2$. Однако по техническим причинам удобно считать главной вторую координату. Говоря о произведении двух линейно упорядоченных множеств как о линейно упорядоченном множестве, мы в дальнейшем подразумеваем именно такой порядок (сначала сравниваем по второй координате).

85. Докажите, что в частично упорядоченном множестве $\mathbb{N} \times \mathbb{N}$ (порядок покоординатный) нет бесконечного подмножества, любые два эле-

мента которого были бы несравнимы. Верно ли аналогичное утверждение для $\mathbb{Z} \times \mathbb{Z}$?

86. Докажите аналогичное утверждение для $\mathbb{N}^k$ (порядок покоординатный).

87. Пусть U — конечное множество из n элементов. Рассмотрим множество $P(U)$ всех подмножеств множества U, упорядоченное по включению. Какова максимально возможная мощность множества $S \subset P(U)$, если индуцированный на S порядок линеен? если никакие два элемента S не сравнимы? (Указание: см. задачу 14.)

88. Сколько существует различных линейных порядков на множестве из n элементов?

89. Докажите, что всякий частичный порядок на конечном множестве можно продолжить до линейного («продолжить» означает, что если $x \leqslant y$ в исходном порядке, то и в новом это останется так).

90. Дано бесконечное частично упорядоченное множество X. Докажите, что в нём всегда найдётся либо бесконечное подмножество попарно несравнимых элементов, либо бесконечное подмножество, на котором индуцированный порядок линеен.

91. (Конечный вариант предыдущей задачи.) Даны целые положительные числа m и n. Докажите, что во всяком частично упорядоченном множестве мощности $mn+1$ можно указать либо $m+1$ попарно несравнимых элементов, либо $n+1$ попарно сравнимых.

92. В строчку написаны $mn+1$ различных чисел. Докажите, что можно часть из них вычеркнуть так, чтобы осталась либо возрастающая последовательность длины $m+1$, либо убывающая последовательность длины $n+1$. (Указание: можно воспользоваться предыдущей задачей.)

93. Рассмотрим семейство всех подмножеств натурального ряда, упорядоченное по включению. Существует ли у него линейно упорядоченное (в индуцированном порядке) подсемейство мощности континуум? Существует ли у него подсемейство мощности континуум, любые два элемента которого несравнимы?

Элемент частично упорядоченного множества называют *наибольшим*, если он больше любого другого элемента, и *максимальным*, если не существует большего элемента. Если множество не является линейно упорядоченным, то это не одно и то же: наибольший элемент автоматически является максимальным, но не наоборот. (Одно дело коробка, в которую помещается любая другая, другое — коробка, которая никуда больше не помещается.)

Легко понять, что наибольший элемент в данном частично упорядоченном множестве может быть только один, в то время как максимальных элементов может быть много.

Аналогично определяют *наименьшие* и *минимальные* элементы.

94. Докажите, что любые два максимальных элемента не сравнимы. Докажите, что в конечном частично упорядоченном множестве X для любого элемента x найдётся максимальный элемент y, больший или равный x.

2.2. Изоморфизмы

Два частично упорядоченных множества называются *изоморфными*, если между ними существует *изоморфизм*, то есть взаимно однозначное соответствие, сохраняющее порядок. (Естественно, что в этом случае они равномощны как множества.) Можно сказать так: биекция $f\colon A \to B$ называется изоморфизмом частично упорядоченных множеств A и B, если

$$a_1 \leqslant a_2 \;\Leftrightarrow\; f(a_1) \leqslant f(a_2)$$

для любых элементов $a_1, a_2 \in A$ (слева знак $\leqslant$ обозначает порядок в множестве A, справа — в множестве B).

Очевидно, что отношение изоморфности рефлексивно (каждое множество изоморфно самому себе), симметрично (если X изоморфно Y, то и наоборот) и транзитивно (два множества, изоморфные третьему, изоморфны между собой). Таким образом, все частично упорядоченные множества разбиваются на классы изоморфных, которые называют *порядковыми типами*. (Правда, как и с мощностями, тут необходима осторожность — изоморфных множеств слишком много, и потому говорить о порядковых типах как множествах нельзя.)

Теорема 12. Конечные линейно упорядоченные множества из одинакового числа элементов изоморфны.

$\triangleleft$ Конечное линейно упорядоченное множество всегда имеет наименьший элемент (возьмём любой элемент; если он не наименьший, возьмём меньший, если и он не наименьший, ещё меньший — и так далее; получим убывающую последовательность $x > y > z > \ldots$, которая рано или поздно должна оборваться). Присвоим наименьшему элементу номер 1. Из оставшихся снова выберем наименьший элемент и присвоим ему номер 2 и так далее. Легко понять, что порядок между элементами соответствует порядку между номерами, то есть что наше множество изоморфно множеству $\{1, 2, \ldots, n\}$. $\triangleright$

95. Докажите, что множество всех целых положительных делителей числа 30 с отношением «быть делителем» в качестве отношения порядка

изоморфно множеству всех подмножеств множества $\{a, b, c\}$, упорядоченному по включению.

96. Будем рассматривать финитные последовательности натуральных чисел, то есть последовательности, у которых все члены, кроме конечного числа, равны 0. На множестве таких последовательностей введём покомпонентный порядок: $(a_0, a_1, \dots) \leqslant (b_0, b_1, \dots)$, если $a_i \leqslant b_i$ при всех i. Докажите, что это множество изоморфно множеству всех положительных целых чисел с отношением «быть делителем» в качестве порядка.

Взаимно однозначное отображение частично упорядоченного множества A в себя, являющееся изоморфизмом, называют *автоморфизмом* частично упорядоченного множества A. Тождественное отображение всегда является автоморфизмом, но для некоторых множеств существуют и другие автоморфизмы. Например, отображение прибавления единицы ($x \mapsto x + 1$) является автоморфизмом частично упорядоченного множества $\mathbb{Z}$ целых чисел (с естественным порядком). Для множества натуральных чисел та же формула не даёт автоморфизма (нет взаимной однозначности).

97. Покажите, что не существует автоморфизма упорядоченного множества $\mathbb{N}$ натуральных чисел, отличного от тождественного.

98. Рассмотрим множество $P(A)$ всех подмножеств некоторого k-элементного множества A, частично упорядоченное по включению. Найдите число автоморфизмов этого множества.

99. Покажите, что множество целых положительных чисел, частично упорядоченное отношением «x делит y», имеет континуум различных автоморфизмов.

Вот несколько примеров равномощных, но не изоморфных линейно упорядоченных множеств (в силу теоремы 12 они должны быть бесконечными).

- Отрезок $[0, 1]$ (с обычным отношением порядка) не изоморфен множеству $\mathbb{R}$, так как у первого есть наибольший элемент, а у второго нет. (При изоморфизме наибольший элемент, естественно, должен соответствовать наибольшему.)

- Множество $\mathbb{Z}$ (целые числа с обычным порядком) не изоморфно множеству $\mathbb{Q}$ (рациональные числа). В самом деле, пусть $\alpha\colon \mathbb{Z} \to \mathbb{Q}$ является изоморфизмом. Возьмём два соседних целых числа, скажем, 2 и 3. При изоморфизме α им должны соответствовать какие-то два рациональных числа $\alpha(2)$ и $\alpha(3)$, причём $\alpha(2) < \alpha(3)$, так как $2 < 3$. Но тогда рациональным числам между $\alpha(2)$ и $\alpha(3)$ должны соответствовать целые числа между 2 и 3, которых нет.

- Более сложный пример — множества $\mathbb{Z}$ и $\mathbb{Z}+\mathbb{Z}$. Возьмём в $\mathbb{Z}+\mathbb{Z}$ две копии нуля (из той и другой компоненты); мы обозначали их 0 и $\overline{0}$. При этом $0 < \overline{0}$. При изоморфизме им должны соответствовать два целых числа a и b, для которых $a < b$. Тогда всем элементам между 0 и $\overline{0}$ (их бесконечно много: $1, 2, 3, \ldots, -\overline{3}, -\overline{2}, -\overline{1}$) должны соответствовать числа между a и b — но их лишь конечное число.

  Этот пример принципиально отличается от предыдущих тем, что здесь разницу между свойствами множеств нельзя записать формулой. Как говорят, упорядоченные множества $\mathbb{Z}$ и $\mathbb{Z}+\mathbb{Z}$ «элементарно эквивалентны».

100. Докажите, что линейно упорядоченные множества $\mathbb{Z}\times\mathbb{N}$ и $\mathbb{Z}\times\mathbb{Z}$ (с описанным выше на с. 46 порядком) не изоморфны.

101. Будут ли изоморфны линейно упорядоченные множества $\mathbb{N}\times\mathbb{Z}$ и $\mathbb{Z}\times\mathbb{Z}$?

102. Будут ли изоморфны линейно упорядоченные множества $\mathbb{Q}\times\mathbb{Z}$ и $\mathbb{Q}\times\mathbb{N}$?

Отображение $x\mapsto\sqrt{2}x$ осуществляет изоморфизм между интервалами $(0,1)$ и $(0,\sqrt{2})$. Но уже не так просто построить изоморфизм между множествами рациональных точек этих интервалов (то есть между $\mathbb{Q}\cap(0,1)$ и $\mathbb{Q}\cap(0,\sqrt{2})$), поскольку умножение на $\sqrt{2}$ переводит рациональные числа в иррациональные. Тем не менее изоморфизм построить можно. Для этого надо взять возрастающие последовательности рациональных чисел $0 < x_1 < x_2 < \ldots$ и $0 < y_1 < y_2 < \ldots$, сходящиеся соответственно к 1 и $\sqrt{2}$, и построить кусочно-линейную функцию f, которая переводит x_i в y_i и линейна на каждом из отрезков $[x_i, x_{i+1}]$ (рис. 5). Легко понять, что она будет искомым изоморфизмом.

103. Покажите, что множество рациональных чисел интервала $(0,1)$ и множество $\mathbb{Q}$ изоморфны. (Указание: здесь тоже можно построить ломаную; впрочем, можно действовать иначе и начать с того, что функция $x\mapsto 1/x$ переводит рациональные числа в рациональные.)

Более сложная конструкция требуется в следующей задаче (видимо, ничего проще, чем сослаться на общую теорему 13, тут не придумаешь).

104. Докажите, что множество двоично-рациональных чисел интервала $(0,1)$ изоморфно множеству $\mathbb{Q}$. (Число считается *двоично-рациональным*, если оно имеет вид $m/2^n$, где m — целое число, а n — натуральное.)

Два элемента x, y линейно упорядоченного множества называют

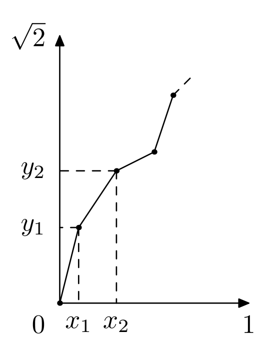


Рис. 5. Ломаная осуществляет изоморфизм.

соседними, если $x < y$ и не существует элемента между ними, то есть такого z, что $x < z < y$. Линейно упорядоченное множество называют *плотным*, если в нём нет соседних элементов (то есть между любыми двумя есть третий).

Теорема 13. Любые два счётных плотных линейно упорядоченных множества без наибольшего и наименьшего элементов изоморфны.

$\triangleleft$ Пусть X и Y — данные нам множества. Требуемый изоморфизм между ними строится по шагам. После n шагов у нас есть два n-элементных подмножества $X_n \subset X$ и $Y_n \subset Y$, элементы которых мы будем называть «охваченными», и взаимно однозначное соответствие между ними, сохраняющее порядок. На очередном шаге мы берём какой-то неохваченный элемент одного из множеств (скажем, множества X) и сравниваем его со всеми охваченными элементами X. Он может оказаться либо меньше всех, либо больше, либо попасть между какими-то двумя. В каждом из случаев мы можем найти неохваченный элемент в Y, находящийся в том же положении (больше всех, между первым и вторым охваченным сверху, между вторым и третьим охваченным сверху и т. п.). При этом мы пользуемся тем, что в Y нет наименьшего элемента, нет наибольшего и нет соседних элементов, — в зависимости от того, какой из трёх случаев имеет место. После этого мы добавляем выбранные элементы к X_n и Y_n, считая их соответствующими друг другу.

Чтобы в пределе получить изоморфизм между множествами X и Y, мы должны позаботиться о том, чтобы все элементы обоих множеств были рано или поздно охвачены. Это можно сделать так: по-

скольку каждое из множеств счётно, пронумеруем его элементы и будем выбирать неохваченный элемент с наименьшим номером (на нечётных шагах — из X, на чётных — из Y). Это соображение завершает доказательство. ▷

105. Сколько существует неизоморфных счётных плотных линейно упорядоченных множеств (про наименьший и наибольший элементы ничего не известно)? (Ответ: 4.)

106. Приведите пример неизоморфных линейно упорядоченных множеств мощности $\mathfrak{c}$ без наименьшего и наибольшего элементов. (Указание: возьмите множества $\mathbb{Q}+\mathbb{R}$ и $\mathbb{R}+\mathbb{Q}$.)

Теорема 14. Всякое счётное линейно упорядоченное множество изоморфно некоторому подмножеству множества $\mathbb{Q}$.

◁ Заметим сразу же, что вместо множества $\mathbb{Q}$ можно было взять любое плотное счётное всюду плотное множество без первого и последнего элементов, так как они все изоморфны.

Доказательство этого утверждения происходит так же, как и в теореме 13 — с той разницей, что новые необработанные элементы берутся только с одной стороны (из данного нам множества), а пары к ним подбираются в множестве рациональных чисел. ▷

107. Дайте другое доказательство теоремы 14, заметив, что любое множество X изоморфно подмножеству множества $\mathbb{Q}\times X$.

2.3. Фундированные множества

Принцип математической индукции в одной из возможных форм звучит так:

> *Пусть $A(n)$ — некоторое свойство натурального числа n. Пусть нам удалось доказать $A(n)$ в предположении, что $A(m)$ верно для всех m, меньших n. Тогда свойство $A(n)$ верно для всех натуральных чисел n.*

(Заметим, что по условию доказательство $A(0)$ возможно без всяких предположений, поскольку меньших чисел нет.)

Для каких частично упорядоченных множеств верен аналогичный принцип? Ответ даётся следующей простой теоремой:

Теорема 15. Следующие три свойства частично упорядоченного множества X равносильны:

(а) любое непустое подмножество X имеет минимальный элемент;

(б) не существует бесконечной строго убывающей последовательности $x_0 > x_1 > x_2 > \ldots$ элементов множества X;

(в) для множества X верен принцип индукции в следующей форме: если (при каждом $x \in X$) из истинности $A(y)$ для всех $y < x$

следует истинность $A(x)$, то свойство $A(x)$ верно при всех x. Формально это записывают так:

$$\forall x\,(\forall y\,((y < x) \Rightarrow A(y)) \Rightarrow A(x)) \Rightarrow \forall x\, A(x).$$

$\lhd$ Сначала докажем эквивалентность первых двух свойств. Если $x_0 > x_1 > x_2 > \ldots$ — бесконечная убывающая последовательность, то, очевидно, множество её значений не имеет минимального элемента (для каждого элемента следующий ещё меньше). Поэтому из (а) следует (б). Напротив, если B — непустое множество, не имеющее минимального элемента, то бесконечную убывающую последовательность можно построить так. Возьмём произвольный элемент $b_0 \in B$. По предположению он не является минимальным, так что можно найти $b_1 \in B$, для которого $b_0 > b_1$. По тем же причинам можно найти $b_2 \in B$, для которого $b_1 > b_2$ и т. д. Получается бесконечная убывающая последовательность.

Теперь выведем принцип индукции из существования минимального элемента в любом подмножестве. Пусть $A(x)$ — произвольное свойство элементов множества X, верное не для всех элементов x. Рассмотрим непустое множество B тех элементов, для которых свойство A неверно. Пусть x — минимальный элемент множества B. По условию меньших элементов в множестве B нет, поэтому для всех $y < x$ свойство $A(y)$ выполнено. Но тогда по предположению должно быть выполнено и $A(x)$ — противоречие.

Осталось доказать существование минимального элемента в любом непустом подмножестве, исходя из принципа индукции. Пусть B — подмножество без минимальных элементов. Докажем по индукции, что B пусто; другими словами, в качестве $A(x)$ возьмём свойство $x \notin B$. В самом деле, если $A(y)$ верно для всех $y < x$, то никакой элемент, меньший x, не лежит в B. Если бы x лежал в B, то он был бы там минимальным, а таких нет. $\rhd$

Множества, обладающие свойствами (а) – (в), называются *фундированными*. Какие есть примеры фундированных множеств? Прежде всего, наш исходный пример — множество натуральных чисел.

Другой пример — множество $\mathbb{N}\times\mathbb{N}$ пар натуральных чисел (меньше та пара, у которой второй член меньше; в случае равенства сравниваем первые). В самом деле, проверим условие (б). Нам будет удобно сформулировать его так: всякая последовательность $u_0 \geqslant u_1 \geqslant u_2 \geqslant \ldots$ элементов множества рано или поздно стабилизируется

(все члены, начиная с некоторого, равны); очевидно, что это эквивалентная формулировка.

Пусть дана произвольная последовательность пар

$$\langle x_0, y_0\rangle \geqslant \langle x_1, y_1\rangle \geqslant \langle x_2, y_2\rangle \geqslant \ldots$$

По определению порядка (сначала сравниваются вторые члены) $y_0 \geqslant \geqslant y_1 \geqslant y_2 \geqslant \ldots$ и потому последовательность натуральных чисел y_i с какого-то места не меняется. После этого уже x_i должны убывать — и тоже стабилизируются. Что и требовалось.

То же самое рассуждение пригодно и в более общей ситуации.

Теорема 16. Пусть A и B — два фундированных частично упорядоченных множества. Тогда их произведение $A \times B$, в котором

$$\langle a_1, b_1\rangle \leqslant \langle a_2, b_2\rangle \Leftrightarrow [(b_1 < b_2) \text{ или } (b_1 = b_2 \text{ и } a_1 \leqslant a_2)],$$

является фундированным.

$\lhd$ В последовательности $\langle a_0, b_0\rangle \geqslant \langle a_1, b_1\rangle \geqslant \ldots$ стабилизируются сначала вторые, а затем и первые члены. $\rhd$

Отсюда вытекает аналогичное утверждение для $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, для $\mathbb{N}^k$ или вообще для произведения конечного числа фундированных множеств.

Ещё проще доказать, что сумма $A+B$ двух фундированных множеств A и B фундирована: последовательность $x_0 \geqslant x_1 \geqslant x_2 \geqslant \ldots$ либо целиком содержится в B (и мы ссылаемся на фундированность B), либо содержит элемент из A. В последнем случае все следующие элементы также принадлежат A, и мы используем фундированность A.

Часто в программировании (или в олимпиадных задачах) нам нужно доказать, что некоторый процесс не может продолжаться бесконечно долго. Например, написав цикл, мы должны убедиться, что рано или поздно из него выйдем. Это можно сделать так: ввести какой-то натуральный параметр и убедиться, что на каждом шаге цикла этот параметр уменьшается. Тогда, если сейчас этот параметр равен N, то можно гарантировать, что не позже чем через N шагов цикл закончится.

Однако бывают ситуации, в которых число шагов заранее оценить нельзя, но тем не менее гарантировать завершение цикла можно, поскольку есть параметр, принимающий значения в фундированном множестве и убывающий на каждом шаге цикла.

Вот пример олимпиадной задачи, где по существу такое рассуждение и используется.

Бизнесмен заключил с чёртом сделку: каждый день он даёт чёрту одну монету, и в обмен получает любой набор монет по своему выбору, но все эти монеты меньшего достоинства (видов монет конечное число). Менять (или получать) деньги в другом месте бизнесмен не может. Когда монет больше не останется, бизнесмен проигрывает. Докажите, что рано или поздно чёрт выиграет, каков бы ни был начальный набор монет у бизнесмена.

Решение: пусть имеется k видов монет. Искомый параметр определим так: посчитаем, сколько монет каждого вида есть у бизнесмена (n_1 — число монет минимального достоинства, n_2 — число следующих, и так далее до n_k). Заметим, что в результате встречи с чёртом набор $\langle n_1, \ldots, n_k \rangle$ уменьшается (в смысле введённого нами порядка, когда мы сравниваем сначала последние члены, затем предпоследние и т. д.). Поскольку множество $\mathbb{N}^k$ фундировано, этот процесс должен оборваться.

108. Имеется конечная последовательность нулей и единиц. За один шаг разрешается сделать такое действие: найти в ней группу 01 и заменить на 100. . .00 (при этом можно написать сколько угодно нулей). Докажите, что такие шаги нельзя выполнять бесконечно много раз.

109. Рассмотрим множество всех слов русского алфавита (точнее, всех конечных последовательностей русских букв, независимо от смысла) с лексикографическим порядком (см. с. 44). Будет ли это множество фундировано?

110. Рассмотрим множество невозрастающих последовательностей натуральных чисел, в которых все члены, начиная с некоторого, равны нулю. Введём в нём порядок так: сначала сравниваем первые члены, при равенстве первых вторые и т. д. Докажите, что это (линейно) упорядоченное множество фундировано.

111. Рассмотрим множество всех многочленов от одной переменной x, коэффициенты которых — натуральные числа. Упорядочим его так: многочлен P больше многочлена Q, если $P(x) > Q(x)$ для всех достаточно больших x. Покажите, что это определение задаёт линейный порядок и что получающееся упорядоченное множество фундировано.

2.4. Вполне упорядоченные множества

Фундированные линейно упорядоченные множества называются *вполне упорядоченными*, а соответствующие порядки — *полными*. Для линейных порядков понятия наименьшего и минимального эле-

мента совпадают, так что во вполне упорядоченном множестве всякое непустое подмножество имеет наименьший элемент.

Заметим, что частично упорядоченное множество, в котором всякое непустое подмножество имеет наименьший элемент, автоматически является линейно упорядоченным (в самом деле, всякое двухэлементное множество имеет наименьший элемент, поэтому любые два элемента сравнимы).

Примеры вполне упорядоченных множеств: $\mathbb{N}$, $\mathbb{N}+k$ (здесь k обозначает конечное линейно упорядоченное множество из k элементов), $\mathbb{N}+\mathbb{N}$, $\mathbb{N}\times\mathbb{N}$.

Наша цель — понять, как могут быть устроены вполне упорядоченные множества. Начнём с нескольких простых замечаний.

- Вполне упорядоченное множество имеет наименьший элемент. (Непосредственное следствие определения.)

- Для каждого элемента x вполне упорядоченного множества (кроме наибольшего) есть непосредственно следующий за ним элемент y (это означает, что $y > x$, но не существует z, для которого $y > z > x$). В самом деле, если множество всех элементов, больших x, непусто, то в нём есть минимальный элемент y, который и будет искомым. Такой элемент обычно обозначают $x+1$, следующий за ним — $x+2$ и т. д.

- Некоторые элементы вполне упорядоченного множества могут не иметь непосредственно предыдущего. Например, в множестве $\mathbb{N}+\mathbb{N}$ есть два элемента, не имеющих непосредственно предыдущего (наименьший элемент, а также наименьший элемент второй копии натурального ряда). Такие элементы называют *предельными*.

- Всякий элемент упорядоченного множества имеет вид $z+n$, где z — предельный, а n — натуральное число (обозначение $z+n$ понимается в описанном выше смысле). В самом деле, если z не предельный, возьмём предыдущий, если и он непредельный — то его предыдущий и т. д., пока не дойдём до предельного (бесконечно продолжаться это не может, так как множество вполне упорядочено). Очевидно, такое представление однозначно (у элемента может быть только один непосредственно предыдущий).

- Любое ограниченное сверху множество элементов вполне упорядоченного множества имеет точную верхнюю грань. (Как обычно, подмножество X частично упорядоченного множества A называется *ограниченным сверху*, если оно имеет *верхнюю границу*, т. е. элемент $a \in A$, для которого $x \leqslant a$ при всех $x \in X$. Если среди всех верхних границ данного подмножества есть наименьшая, то она называется *точной верхней гранью*.)

  В самом деле, множество всех верхних границ непусто и потому имеет наименьший элемент. (Заметим в скобках, что вопрос о точной нижней грани для вполне упорядоченного множества тривиален, так как всякое множество имеет наименьший элемент.)

Пусть A — произвольное вполне упорядоченное множество. Его наименьший элемент обозначим через 0. Следующий за ним элемент обозначим через 1, следующий за 1 — через 2 и т. д. Если множество конечно, процесс этот оборвётся. Если бесконечно, посмотрим, исчерпали ли мы все элементы множества A. Если нет, возьмём минимальный элемент из оставшихся. Обозначим его ω. Следующий за ним элемент (если он есть) обозначим $\omega+1$, затем $\omega+2$ и т. д. Если и на этом множество не исчерпается, то возьмём наименьший элемент из оставшихся, назовём его $\omega \cdot 2$, и повторим всю процедуру. Затем будут $\omega \cdot 3$, $\omega \cdot 4$ и т. д. Если и на этом множество не кончится, минимальный из оставшихся элементов назовём ω^2. Затем пойдут ω^2+1, $\omega^2+2, \ldots, \omega^2+\omega, \ldots, \omega^2+\omega \cdot 2, \ldots, \omega^2 \cdot 2, \ldots, \omega^2 \cdot 3, \ldots, \omega^3, \ldots$ (мы не поясняем сейчас подробно обозначения).

Что, собственно говоря, доказывает это рассуждение? Попытаемся выделить некоторые утверждения. При этом полезно такое определение: если линейно упорядоченное множество A разбито на две (непересекающиеся) части B и C, причём любой элемент B меньше любого элемента C, то B называют *начальным отрезком* множества A. Другими словами, подмножество B линейно упорядоченного множества A является начальным отрезком, если любой элемент B меньше любого элемента $A \setminus B$. Ещё одна переформулировка: $B \subset A$ является начальным отрезком, если из $a, b \in A$, $b \in B$ и $a \leqslant b$ следует $a \in B$. Заметим, что начальный отрезок может быть пустым или совпадать со всем множеством.

Отметим сразу же несколько простых свойств начальных отрезков:

- Начальный отрезок вполне упорядоченного множества (как, впрочем, и любое подмножество) является вполне упорядоченным множеством.

- Начальный отрезок начального отрезка есть начальный отрезок исходного множества.

- Объединение любого семейства начальных отрезков (в одном и том же упорядоченном множестве) есть начальный отрезок того же множества.

- Если x — произвольный элемент вполне упорядоченного множества A, то множества $[0, x)$ (все элементы множества A, меньшие x) и $[0, x]$ (элементы множества A, меньшие или равные x) являются начальными отрезками.

- Всякий начальный отрезок I вполне упорядоченного множества A, не совпадающий со всем множеством, имеет вид $[0, x)$ для некоторого $x \in A$. (В самом деле, если $I \neq A$, возьмём наименьший элемент x в множестве $A \setminus I$. Тогда все меньшие элементы принадлежат I, сам x не принадлежит I и все бо́льшие x элементы не принадлежат I, иначе получилось бы противоречие с определением начального отрезка.)

- Любые два начальных отрезка вполне упорядоченного множества сравнимы по включению, т. е. один есть подмножество другого. (Следует из предыдущего.)

- Начальные отрезки вполне упорядоченного множества A, упорядоченные по включению, образуют вполне упорядоченное множество. Это множество состоит из наибольшего элемента (всё A) и остальной части, изоморфной множеству A. (В самом деле, начальные отрезки множества A, не совпадающие с A, имеют вид $[0, x)$, и соответствие $[0, x) \leftrightarrow x$ будет изоморфизмом.)

Возвратимся к нашему рассуждению с последовательным выделением различных элементов из вполне упорядоченного множества. Его первую часть можно считать доказательством такого утверждения: если вполне упорядоченное множество бесконечно, то оно имеет начальный отрезок, изоморфный ω. (Говоря о множестве натуральных чисел вместе с порядком, обычно употребляют обозначение ω, а не $\mathbb{N}$.)

Но на этом наше рассуждение не оканчивается. Его следующая часть может считаться доказательством такого факта: либо A изоморфно некоторому начальному отрезку множества ω^2, либо оно имеет начальный отрезок, изоморфный ω^2. (Здесь ω^2 — вполне упорядоченное множество пар натуральных чисел: сравниваются сначала вторые компоненты пар, а при их равенстве — первые.)

Вообще верно такое утверждение: для любых двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого, и доказательство состоит более или менее в повторении проведённого рассуждения. Но чтобы сделать это аккуратно, нужна некоторая подготовка.

2.5. Трансфинитная индукция

Термины «индукция» и «рекурсия» часто употребляются вперемежку. Например, определение факториала $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ как функции $f(n)$, для которой $f(n) = n \cdot f(n-1)$ при $n > 0$ и $f(0) = 1$, называют и «индуктивным», и «рекурсивным». Мы будем стараться разграничивать эти слова так: если речь идёт о доказательстве чего-то сначала для $n = 0$, затем для $n = 1, 2, \ldots$, причём каждое утверждение опирается на предыдущее, то это *индукция*. Если же мы определяем что-то сначала для $n = 0$, потом для $n = 1, 2, \ldots$, причём определение каждого нового значения использует ранее определённые, то это *рекурсия*.

Наша цель — научиться проводить индуктивные доказательства и давать рекурсивные определения не только для натуральных чисел, но и для других вполне упорядоченных множеств.

Доказательства по индукции мы уже обсуждали, говоря о фундированных множествах (см. раздел 2.3), и сейчас ограничимся только одним примером.

Теорема 17. Пусть множество A вполне упорядочено, а отображение $f\colon A \to A$ возрастает (то есть $f(x) < f(y)$ при $x < y$). Тогда $f(x) \geqslant x$ для всех $x \in A$.

$\lhd$ Согласно принципу индукции (теорема 15, с. 52) достаточно доказать неравенство $f(x) \geqslant x$, предполагая, что $f(y) \geqslant y$ при всех $y < x$. Пусть это не так и $f(x) < x$. Тогда по монотонности $f(f(x)) < f(x)$. Но, с другой стороны, элемент $y = f(x)$ меньше x, и потому по предположению индукции $f(y) \geqslant y$, то есть $f(f(x)) \geqslant f(x)$.

Если угодно, можно в явном виде воспользоваться существованием наименьшего элемента и изложить это же рассуждение так. Пусть

утверждение теоремы неверно. Возьмём наименьшее x, для которого $f(x) < x$. Но тогда $f(f(x)) < f(x)$ по монотонности и потому x не является наименьшим вопреки предположению.

Наконец, это рассуждение можно пересказать и так: если $x > f(x)$, то по монотонности

$$x > f(x) > f(f(x)) > f(f(f(x))) > \ldots,$$

но бесконечных убывающих последовательностей в фундированном множестве быть не может. $\triangleright$

Теперь перейдём к рекурсии. В определении факториала $f(n)$ выражалось через $f(n-1)$. В общей ситуации значение $f(n)$ может использовать не только одно предыдущее значение функции, но и все значения на меньших аргументах. Например, можно определить функцию $f\colon \mathbb{N} \to \mathbb{N}$, сказав, что $f(n)$ на единицу больше суммы всех предыдущих значений, то есть $f(n) = f(0) + f(1) + \ldots + f(n-1) + 1$; это вполне законное рекурсивное определение (надо только пояснить, что пустая сумма считается равной нулю, так что $f(0) = 1$).

112. Какую функцию f задаёт такое определение?

Как обобщить эту схему на произвольные вполне упорядоченные множества вместо натурального ряда? Пусть A вполне упорядочено. Мы хотим дать рекурсивное определение функции $f\colon A \to B$ (где B — некоторое множество). Такое определение должно связывать значение $f(x)$ на некотором элементе $x \in A$ со значениями $f(y)$ при всех $y < x$. Другими словами, рекурсивное определение указывает $f(x)$, предполагая известным ограничение функции f на начальный отрезок $[0, x)$. Вот точная формулировка:

Теорема 18. Пусть A — вполне упорядоченное множество. Пусть B — произвольное множество. Пусть имеется некоторое рекурсивное правило, то есть отображение F, которое ставит в соответствие элементу $x \in A$ и функции $g\colon [0, x) \to B$ некоторый элемент множества B. Тогда существует и единственна функция $f\colon A \to B$, для которой

$$f(x) = F(x, f|_{[0,x)})$$

при всех $x \in A$. (Здесь $f|_{[0,x)}$ обозначает ограничение функции f на начальный отрезок $[0, x)$ — мы отбрасываем все значения функции на элементах, больших или равных x.)

$\triangleleft$ Неформально можно рассуждать так: значение f на минимальном элементе определено однозначно, так как предыдущих значений

нет (сужение $f|_{[0,0)}$ пусто). Тогда и на следующем элементе значение функции f определено однозначно, поскольку на предыдущих (точнее, единственном предыдущем) функция f уже задана, и т. д.

Конечно, это надо аккуратно выразить формально. Вот как это делается. Докажем по индукции такое утверждение о произвольном элементе $a \in A$:

> *существует и единственно отображение f отрезка $[0, a]$ в множество B, для которого рекурсивное определение* (*равенство, приведённое в условии*) *выполнено при всех $x \in [0, a]$.*

Будем называть отображение $f\colon [0, a] \to B$, обладающее указанным свойством, *корректным.* Таким образом, мы хотим доказать, что для каждого $a \in A$ есть единственное корректное отображение отрезка $[0, a]$ в B.

Поскольку мы рассуждаем по индукции, можно предполагать, что для всех $c < a$ это утверждение выполнено, то есть существует и единственно корректное отображение $f_c\colon [0, c] \to B$. (Корректность f_c означает, что при всех $d \leqslant c$ значение $f_c(d)$ совпадает с предписанным по рекурсивному правилу.)

Рассмотрим отображения f_{c_1} и f_{c_2} для двух различных c_1 и c_2. Пусть, например, $c_1 < c_2$. Отображение f_{c_2} определено на большем отрезке $[0, c_2]$. Если ограничить f_{c_2} на меньший отрезок $[0, c_1]$, то оно совпадёт с f_{c_1}, поскольку ограничение корректного отображения на меньший отрезок корректно (это очевидно), а мы предполагали единственность на отрезке $[0, c_1]$.

Таким образом, все отображения f_c согласованы друг с другом, то есть принимают одинаковое значение, если определены одновременно. Объединив их, мы получаем некоторое единое отображение h, определённое на $[0, a)$. Применив к a и h рекурсивное правило, получим некоторое значение $b \in B$. Доопределим h в точке a, положив $h(a) = b$. Получится отображение $h\colon [0, a] \to B$; легко понять, что оно корректно.

Чтобы завершить индуктивный переход, надо проверить, что на отрезке $[0, a]$ корректное отображение единственно. В самом деле, его ограничения на отрезки $[0, c]$ при $c < a$ должны совпадать с f_c, поэтому осталось проверить однозначность в точке a — что гарантируется рекурсивным определением (выражающим значение в точке a через предыдущие). На этом индуктивное доказательство заканчивается.

Осталось лишь заметить, что для разных a корректные отобра-

жения отрезков $[0, a]$ согласованы друг с другом (сужение корректного отображения на меньший отрезок корректно, применяем единственность) и потому вместе задают некоторую функцию $f\colon A \to B$, удовлетворяющую рекурсивному определению.

Существование доказано; единственность тоже понятна, так как ограничение этой функции на любой отрезок $[0, a]$ корректно и потому однозначно определено, как мы видели. $\triangleright$

Прежде чем применить эту теорему и доказать, что из двух вполне упорядоченных множеств одно является отрезком другого, нам потребуется её немного усовершенствовать. Нам надо предусмотреть ситуацию, когда рекурсивное правило не всюду определено. Пусть, например, мы определяем последовательность действительных чисел соотношением $x_n = \operatorname{tg} x_{n-1}$ и начальным условием $x_0 = a$. При некоторых значениях a может оказаться, что построение последовательности обрывается, поскольку тангенс не определён для соответствующего аргумента.

113. Докажите, что множество всех таких «исключительных» a (когда последовательность конечна) счётно.

Аналогичная ситуация возможна и для общего случая.

Теорема 19. Пусть отображение F, о котором шла речь в теореме 18, является частичным (для некоторых элементов x и функций $g\colon [0, x) \to B$ оно может быть не определено). Тогда существует функция f, которая

- либо определена на всём A и согласована с рекурсивным определением;
- либо определена на некотором начальном отрезке $[0, a)$ и на нём согласована с рекурсивным определением, причём для точки a и функции f рекурсивное правило неприменимо (отображение F не определено).

$\triangleleft$ Это утверждение является обобщением, но одновременно и следствием предыдущей теоремы 18. В самом деле, добавим к множеству B специальный элемент $\bot$ («неопределённость») и модифицируем рекурсивное правило: новое правило даёт значение $\bot$, когда старое было не определено. (Если среди значений функции на предыдущих аргументах уже встречалось $\bot$, новое рекурсивное правило тоже даёт $\bot$.)

Применив теорему 18 к модифицированному правилу, получим некоторую функцию f'. Если эта функция нигде не принимает зна-

чения $\perp$, то реализуется первая из двух возможностей, указанных в теореме (при $f = f'$). Если же функция f' принимает значение $\perp$ в какой-то точке, то она имеет то же значение $\perp$ и во всех больших точках. Заменив значение $\perp$ на неопределённость, мы получаем из функции f' функцию f. Область определения функции f есть некоторый начальный отрезок $[0, a)$ и реализуется вторая возможность, указанная в формулировке теоремы. $\triangleright$

114. Сформулируйте и докажите утверждение об однозначности функции, заданной частичным рекурсивным правилом.

Теперь у нас всё готово для доказательства теоремы о сравнении вполне упорядоченных множеств.

Теорема 20. Пусть A и B — два вполне упорядоченных множества. Тогда либо A изоморфно некоторому начальному отрезку множества B, либо B изоморфно некоторому начальному отрезку множества A.

$\triangleleft$ Отметим прежде всего, что начальный отрезок может совпадать со всем множеством, так что случай изоморфных множеств A и B также покрывается этой теоремой.

Определим отображение f из A в B таким рекурсивным правилом: для любого $a \in A$

> *$f(a)$ есть наименьший элемент множества B, который не встречается среди $f(a')$ при $a' < a$.*

Это правило не определено в том случае, когда значения $f(a')$ при $a' < a$ покрывают всё B. Применяя теорему 19, мы получаем функцию f, согласованную с этим правилом. Теперь рассмотрим два случая:

- Функция f определена на всём A. Заметим, что рекурсивное определение гарантирует монотонность, поскольку $f(a)$ определяется как минимальный ещё не использованный элемент; чем больше a, тем меньше остаётся неиспользованных элементов и потому минимальный элемент может только возрасти (из определения следует также, что одинаковых значений быть не может). Остаётся лишь проверить, что множество значений функции f, то есть $f(A)$, будет начальным отрезком. В самом деле, пусть $b < f(a)$ для некоторого $a \in A$; надо проверить, что b также является значением функции f. Действительно, согласно рекурсивному определению $f(a)$ является наименьшим неиспользованным значением, следовательно, b уже использовано, то есть встречается среди $f(a')$ при $a' < a$.

- Функция f определена лишь на некотором начальном отрезке $[0, a)$. В этом случае этот начальный отрезок изоморфен B, и функция f является искомым изоморфизмом. В самом деле, раз $f(a)$ не определено, то среди значений функции f встречаются все элементы множества B. С другой стороны, f сохраняет порядок в силу рекурсивного определения.

Таким образом, в обоих случаях утверждение теоремы верно. $\triangleright$

Может ли быть так, что A изоморфно начальному отрезку B, а B изоморфно начальному отрезку A? Нет — за исключением тривиального случая, когда начальные отрезки представляют собой сами множества A и B. Это вытекает из такого утверждения:

Теорема 21. Никакое вполне упорядоченное множество не изоморфно своему начальному отрезку (не совпадающему со всем множеством).

$\triangleleft$ Пусть вполне упорядоченное множество A изоморфно своему начальному отрезку, не совпадающему со всем множеством. Как мы видели на с. 58, этот отрезок имеет вид $[0, a)$ для некоторого элемента $a \in A$. Пусть $f\colon A \to [0, a)$ — изоморфизм. Тогда f строго возрастает, и по теореме 17 имеет место неравенство $f(a) \geqslant a$, что противоречит тому, что множество значений функции f есть $[0, a)$. $\triangleright$

Если множество A изоморфно начальному отрезку множества B, а множество B изоморфно начальному отрезку множества A, то композиция этих изоморфизмов даёт изоморфизм между множеством A и его начальным отрезком (начальный отрезок начального отрезка есть начальный отрезок). Этот начальный отрезок обязан совпадать со всем множеством A, так что это возможно лишь если A и B изоморфны.

Сказанное позволяет сравнивать вполне упорядоченные множества. Если A изоморфно начальному отрезку множества B, не совпадающему со всем B, то говорят, что *порядковый тип множества A меньше порядкового типа множества B*. Если множества A и B изоморфны, то говорят, что у них *одинаковые порядковые типы*. Наконец, если B изоморфно начальному отрезку множества A, то говорят, что *порядковый тип множества A больше порядкового типа множества B*. Как мы только что доказали, верно такое утверждение:

Теорема 22. Для любых вполне упорядоченных множеств A и B имеет место ровно один из указанных трёх случаев.

Если временно забыть о проблемах оснований теории множеств

и определить порядковый тип упорядоченного множества как класс изоморфных ему упорядоченных множеств, то можно сказать, что мы определили линейный порядок на порядковых типах вполне упорядоченных множеств (на *ординалах*, как говорят). Этот порядок будет полным. Мы переформулируем это утверждение так, чтобы избегать упоминания классов.

Теорема 23. Всякое непустое семейство вполне упорядоченных множеств имеет «наименьший элемент» — множество, изоморфное начальным отрезкам всех остальных множеств.

$\triangleleft$ Возьмём какое-то множество X семейства. Если оно наименьшее, то всё доказано. Если нет, рассмотрим все множества семейства, которые меньше его, то есть изоморфны его начальным отрезкам вида $[0, x)$. Среди всех таких элементов x выберем наименьший. Тогда соответствующее ему множество и будет наименьшим. $\triangleright$

Следствием доказанных теорем является то, что любые два вполне упорядоченных множества сравнимы по мощности (одно равномощно подмножеству другого). Сейчас мы увидим, что всякое множество может быть вполне упорядочено (теорема Цермело), и, следовательно, любые два множества сравнимы по мощности.

2.6. Теорема Цермело

Теорема 24 (Цермело). Всякое множество может быть вполне упорядочено.

$\triangleleft$ Доказательство этой теоремы существенно использует аксиому выбора и вызывало большие нарекания своей неконструктивностью. На счётных множествах полный порядок указать легко (перенеся с $\mathbb{N}$). Но уже на множестве действительных чисел никакого конкретного полного порядка указать не удаётся, и доказав (с помощью аксиомы выбора) его существование, мы так и не можем себе этот порядок представить.

Объясним, в какой форме используется аксиома выбора. Пусть A — данное нам множество. Мы принимаем, что существует функция φ, определённая на всех подмножествах множества A, кроме самого́ A, которая указывает один из элементов вне этого подмножества:

$$X \subsetneq A \Rightarrow \varphi(X) \in A \setminus X.$$

После того как такая функция фиксирована, можно построить полный порядок на A, и в этом построении уже нет никакой неоднозначности. Вот как это делается.

Наименьшим элементом множества A мы объявим элемент $a_0 = \varphi(\varnothing)$. За ним идёт элемент $a_1 = \varphi(\{a_0\})$; по построению он отличается от a_0. Далее следует элемент $a_2 = \varphi(\{a_0, a_1\})$. Если множество A бесконечно, то такой процесс можно продолжать и получить последовательность $\{a_0, a_1, \ldots\}$ элементов множества A. Если после этого остаются ещё не использованные элементы множества A, рассмотрим элемент $a_\omega = \varphi(\{a_0, a_1, a_2, \ldots\})$ и так будем продолжать, пока всё A не кончится; когда оно кончится, порядок выбора элементов и будет полным порядком на A.

Конечно, последняя фраза нуждается в уточнении — что значит «так будем продолжать»? Возникает желание применить теорему о трансфинитной рекурсии (у нас очень похожая ситуация: следующий элемент определяется рекурсивно, если известны все предыдущие). И это можно сделать, если у нас есть другое вполне упорядоченное множество B, и получить взаимно однозначное соответствие либо между A и частью B, либо между B и частью A. В первом случае всё хорошо, но для этого надо иметь вполне упорядоченное множество B по крайней мере той же мощности, что и A, так что получается некий порочный круг.

Тем не менее из него можно выйти. Мы сделаем это так: рассмотрим все потенциальные кусочки будущего порядка и убедимся, что их можно склеить.

Пусть $(S, \leqslant_S)$ — некоторое подмножество множества A и заданный на нём порядок. Будем говорить, что $(S, \leqslant_S)$ является *корректным фрагментом*, если оно является вполне упорядоченным множеством, причём

$$s = \varphi([0, s))$$

для любого $s \in S$. Здесь $[0, s)$ — начальный отрезок множества S, состоящий из всех элементов, меньших s с точки зрения заданного на S порядка.

Например, множество $\{\varphi(\varnothing)\}$ является корректным фрагментом (порядок здесь можно не указывать, так как элемент всего один). Множество $\{\varphi(\varnothing), \varphi(\{\varphi(\varnothing)\})\}$ (первый из выписанных элементов считается меньшим второго) также является корректным фрагментом. Это построение можно продолжать и дальше, но нам надо каким-то образом «перескочить» через бесконечное (и очень большое в смысле мощности) число шагов этой конструкции.

План такой: мы докажем, что любые два корректных фрагмента в определённом смысле согласованы, после чего рассмотреть объеди-

нение всех корректных фрагментов. Оно будет корректным и будет совпадать со всем множеством A (в противном случае его можно было бы расширить и получить корректный фрагмент, не вошедший в объединение).

Лемма 1. Пусть $(S, \leqslant_S)$ и $(T, \leqslant_T)$ — два корректных фрагмента. Тогда один из них является начальным отрезком другого, причём порядки согласованы (два общих элемента всё равно как сравнивать — в смысле $\leqslant_S$ или в смысле $\leqslant_T$).

Заметим, что по теореме 20 один из фрагментов *изоморфен* начальному отрезку другого. Пусть S изоморфен начальному отрезку T и $h\colon S \to T$ — их изоморфизм. Лемма утверждает, что изоморфизм h является тождественным, то есть что $h(x) = x$ при всех $x \in S$. Докажем это индукцией по $x \in S$ (это законно, так как S вполне упорядочено по определению корректного фрагмента). Индуктивное предположение гарантирует, что $h(y) = y$ для всех $y < x$. Мы хотим доказать, что $h(x) = x$. Рассмотрим начальные отрезки $[0, x)_S$ и $[0, h(x))_T$ (с точки зрения порядков $\leqslant_S$ и $\leqslant_T$ соответственно). Они соответствуют друг другу при изоморфизме h, поэтому по предположению индукции совпадают как множества. Но по определению корректности $x = \varphi([0, x))$ и $h(x) = \varphi([0, h(x)))$, так что $x = h(x)$. Лемма 1 доказана.

Рассмотрим объединение всех корректных фрагментов (как множеств). На этом объединении естественно определён линейный порядок: для всяких двух элементов найдётся фрагмент, которому они оба принадлежат (каждый принадлежит своему, возьмём больший из фрагментов), так что их можно сравнить. По лемме 1 порядок не зависит от того, какой фрагмент будет выбран для сравнения.

Лемма 2. Это объединение будет корректным фрагментом.

Чтобы доказать лемму 2, заметим, что на этом объединении определён линейный порядок. Он будет полным. Для разнообразия объясним это в терминах убывающих (невозрастающих) последовательностей. Пусть $x_0 \geqslant x_1 \geqslant \ldots$; возьмём корректный фрагмент F, которому принадлежит x_0. Из леммы 1 следует, что все x_i также принадлежат этому фрагменту (поскольку фрагмент F будет начальным отрезком в любом большем фрагменте), а F вполне упорядочен по определению, так что последовательность стабилизируется. Лемма 2 доказана.

Утверждение леммы 2 можно переформулировать таким образом: существует наибольший корректный фрагмент. Осталось доказать, что этот фрагмент (обозначим его S) включает в себя всё

множество A. Если $S \neq A$, возьмём элемент $a = \varphi(S)$, не принадлежащий S, и добавим его к S, считая, что он больше всех элементов S. Полученное упорядоченное множество S' (сумма S и одноэлементного множества) будет, очевидно, вполне упорядочено. Кроме того, условие корректности также выполнено (для a — по построению, для остальных элементов — поскольку оно было выполнено в S). Таким образом, мы построили больший корректный фрагмент, что противоречит максимальности S. Это рассуждение завершает доказательство теоремы Цермело. $\triangleright$

Как мы уже говорили, из теоремы Цермело и теоремы 20 о сравнении вполне упорядоченных множеств немедленно вытекает такое утверждение:

Теорема 25. Из любых двух множеств одно равномощно подмножеству другого.

Понятие вполне упорядоченного множества ввёл Кантор в работе 1883 года; в его итоговой работе 1895–1897 годов приводится доказательство того, что любые два вполне упорядоченных множества сравнимы (одно изоморфно начальному отрезку другого).

Утверждения о возможности полного упорядочения любого множества и о сравнении мощностей (теоремы 24 и 25) неоднократно встречаются в работах Кантора, но никакого внятного доказательства он не предложил, и оно было дано лишь в 1904 году немецким математиком Э. Цермело.

2.7. Трансфинитная индукция и базис Гамеля

Вполне упорядоченные множества и теорема Цермело позволяют продолжать индуктивные построения в трансфинитную область (если выражаться торжественно). Поясним это на примере из линейной алгебры.

Всякое линейно независимое множество векторов в конечномерном пространстве может быть дополнено до базиса. Как это доказывается? Пусть S — данное нам линейно независимое множество. Если оно не является базисом, то некоторый вектор x_0 через него не выражается. Добавим его к S, получим линейно независимое множество $S \cup \{x_0\}$. Если и оно не является базисом, то некоторый вектор x_1 через него не выражается, и т. д. Либо на каком-то шаге мы получим базис, либо процесс не оборвётся и мы получим бесконечную последовательность линейно независимых векторов, что противоречит конечномерности.

Теперь с помощью трансфинитной индукции (точнее, рекурсии) мы избавимся от требования конечномерности.

Пусть дано произвольное векторное пространство. Говорят, что множество (возможно, бесконечное) векторов *линейно независимо*, если никакая нетривиальная линейная комбинация конечного числа векторов из этого множества не равна нулю. (Заметим в скобках, что говорить о бесконечных линейных комбинациях в принципе можно лишь если в пространстве определена сходимость, чего мы сейчас не предполагаем.) Линейно независимое множество векторов называется *базисом Гамеля* (или просто *базисом*) данного пространства, если любой вектор представим в виде конечной линейной комбинации элементов этого множества.

Как и в конечной ситуации, максимальное линейно независимое множество (которое становится линейно зависимым при добавлении любого нового элемента) является, очевидно, базисом.

Теорема 26. Всякое линейно независимое множество векторов может быть расширено до базиса Гамеля.

$\triangleleft$ Пусть S — линейно независимое подмножество векторного пространства V. Рассмотрим вполне упорядоченное множество I достаточно большой мощности (большей, чем мощность пространства V). Определим функцию f из I в V с помощью трансфинитной рекурсии:

> *$f(i)$ = элемент пространства V, не выражающийся линейно через элементы S и значения $f(j)$ при $j < i$.*

Заметим, что это рекурсивное правило оставляет $f(i)$ неопределённым, если такого невыразимого элемента не существует. (Кроме того, можно отметить, что мы снова используем аксиому выбора. Более подробно следовало бы сказать так: по аксиоме выбора существует некоторая функция, которая по каждому подмножеству пространства V, через которое не всё V выражается, указывает один из невыразимых элементов. Затем эта функция используется в рекурсивном определении. Впрочем, аксиома выбора и так уже использована для доказательства теоремы Цермело.)

Это определение гарантирует, что f является инъекцией; более того можно утверждать, что все значения f вместе с множеством S образуют линейно независимое множество. В самом деле, пусть линейная комбинация некоторых значений функции f и элементов множества S равна нулю. Можно считать, что все коэффициенты в этой комбинации отличны от нуля (отбросив нулевые слагаемые). Входящие в комбинацию значения функции f имеют вид $f(i)$ при различных i. Посмотрим на тот из них, который имеет наибольшее i;

по построению он должен быть линейно независим от остальных — противоречие.

Поскольку мы предположили, что множество I имеет большую мощность, чем V, рекурсивное определение задаёт функцию не на всём I, а только на некотором начальном отрезке $[0,i)$, а в точке i рекурсивное правило не определено (теорема 19). Это означает, что все векторы пространства V выражаются через элементы множества S и значения функции f на промежутке $[0,i)$. Кроме того, как мы видели, все эти векторы независимы. Таким образом, искомый базис найден. $\triangleright$

На самом деле можно обойтись без множества большей мощности, упорядочив само пространство V. При этом на каждом шаге рекурсии надо либо добавлять очередной элемент к будущему базису (если он не выражается через предыдущие), либо оставлять базис без изменений.

115. Проведите это рассуждение подробно.

Базис Гамеля может быть использован для построения разных экзотических примеров. Вот некоторые из них:

Теорема 27. Существует (всюду определённая) функция $f\colon \mathbb{R}\to\mathbb{R}$, для которой $f(x+y)=f(x)+f(y)$ при всех x и y, но которая не есть умножение на константу.

$\triangleleft$ Рассмотрим $\mathbb{R}$ как векторное пространство над полем $\mathbb{Q}$. В нём есть базис Гамеля. Пусть α — один из векторов базиса. Рассмотрим функцию f, которая с каждым числом x (рассматриваемым как вектор в пространстве $\mathbb{R}$ над полем $\mathbb{Q}$) сопоставляет его α-координату (коэффициент при α в единственном выражении x через векторы базиса). Эта функция линейна над $\mathbb{Q}$, поэтому $f(x+y)=f(x)+f(y)$ для всех $x,y\in\mathbb{R}$. Она отлична от нуля ($f(\alpha)=1$) и принимает лишь рациональные значения, поэтому не может быть умножением на константу. $\triangleright$

116. Покажите, что всякая функция, обладающая указанными в теореме 27 свойствами, не ограничена ни на каком отрезке и, более того, её график всюду плотен в $\mathbb{R}^2$.

Теорема 28. Аддитивные группы $\mathbb{R}$ и $\mathbb{R}\oplus\mathbb{R}$ изоморфны.

$\triangleleft$ Рассмотрим $\mathbb{R}$ как векторное пространство над $\mathbb{Q}$ и выберем базис в этом пространстве. Очевидно, он бесконечен. Базис в $\mathbb{R}\oplus\mathbb{R}$ может быть составлен из двух частей, каждая из которых представляет собой базис в одном из экземпляров $\mathbb{R}$. Как мы увидим чуть позже (см. раздел 2.9), для любого бесконечного множества B удво-

енная мощность B (мощность объединения двух непересекающихся множеств, равномощных B) равна мощности B. Наконец, осталось заметить, что пространства над одним и тем же полем с равномощными базисами изоморфны как векторные пространства и тем более как группы. ▷

117. Докажите, что любой базис в пространстве $\mathbb{R}$ над полем $\mathbb{Q}$ имеет мощность континуума. (При доказательстве пригодятся результаты раздела 2.9.)

Мы видели, что трансфинитная индукция позволяет доказать существование базиса в любом векторном пространстве. Продолжая эту линию, можно доказать, что любые два базиса векторного пространства равномощны. (Таким образом, понятие размерности как мощности базиса корректно определено и для бесконечномерных векторных пространств.) Мы вернёмся к этому позже, на с. 83 (теорема 36).

Отметим, что существование базиса Гамеля можно использовать и «в мирных целях», а не только для построения экзотических примеров. Известная «третья проблема Гильберта» состояла в доказательстве того, что многогранники равного объёма могут не быть равносоставлены. (Это значит, что один из них нельзя разрезать на меньшие многогранники и сложить из них другой многогранник.) Для многоугольников на плоскости ситуация иная: если два многоугольника равновелики (имеют равную площадь), то они равносоставлены.

Теорема 29. Куб нельзя разрезать на части, из которых можно было бы составить правильный тетраэдр (независимо от объёма последнего).

◁ Введём понятие *псевдообъёма* многогранника. Как и объём, псевдообъём будет аддитивен (если многогранник разбит на части, сумма их псевдообъёмов равна псевдообъёму исходного многогранника); псевдообъёмы равных многогранников будут равны. Отсюда следует, что псевдообъёмы равносоставленных многогранников будут равны. Мы подберём псевдообъём так, чтобы у куба он равнялся нулю, а у тетраэдра нет — и доказательство будет завершено.

Псевдообъём многогранника мы определим как сумму $\sum l_i\varphi(\alpha_i)$, где сумма берётся по всем рёбрам многогранника, l_i — длина i-го ребра, α_i — двугранный угол при этом ребре, а φ — некоторая функция. Такое определение автоматически гарантирует, что равные многогранники имеют равные псевдообъёмы. Что нужно от функции φ,

чтобы псевдообъём был аддитивен? Представим себе, что многогранник разрезается плоскостью на две части, и плоскость проходит через уже имеющееся ребро длины l. Тогда двугранный угол α при этом ребре разбивается на две части β и γ. Поэтому в выражении для псевдообъёма вместо слагаемого $l\varphi(\alpha)$ появляются слагаемые $l\varphi(\beta) + l\varphi(\gamma)$, и $\varphi(\alpha)$ должно равняться $\varphi(\beta) + \varphi(\gamma)$. Кроме того, разрезающая плоскость может образовать новое ребро, пересекшись с какой-то гранью. Обозначим длину этого ребра за l'. Тогда в псевдообъёме появятся слагаемые $l'\varphi(\alpha)+l'\varphi(\pi-\alpha)$ (два образовавшихся двугранных угла дополнительны), которые в сумме должны равняться нулю.

Теперь ясно, какими свойствами должна обладать функция φ. Нужно, чтобы $\varphi(\beta + \gamma) = \varphi(\beta) + \varphi(\gamma)$ и чтобы $\varphi(\pi) = 0$. Тогда псевдообъём будет и впрямь аддитивен. Аккуратная проверка требует точного определения понятия многогранника (что не так и просто), и мы её проводить не будем. Наглядно аддитивность кажется очевидной, особенно если учесть, что все разрезы можно проводить плоскостями (при этом могут получиться более мелкие части, но это не страшно).

Итак, для завершения рассуждения достаточно построить функцию $\varphi\colon \mathbb{R} \to \mathbb{R}$, для которой

- $\varphi(\beta + \gamma) = \varphi(\beta) + \varphi(\gamma)$ для всех $\beta, \gamma \in \mathbb{R}$;
- $\varphi(\pi) = 0$ (это свойство вместе с предыдущим гарантирует аддитивность псевдообъёма);
- $\varphi(\pi/2) = 0$ (псевдообъём куба равен нулю; это свойство, впрочем, легко следует из двух предыдущих);
- $\varphi(\theta) \neq 0$, где θ — двугранный угол при ребре правильного тетраэдра.

Существенно здесь то, что отношение θ/π иррационально. Проверим это. Высоты двух соседних граней, опущенные на общее ребро, образуют равнобедренный треугольник со сторонами $\sqrt{3}$, $\sqrt{3}$, 2; надо доказать, что углы этого треугольника несоизмеримы с π. Удобнее рассмотреть не θ, а другой угол треугольника (два других угла треугольника равны); обозначим его β. Это угол прямоугольного треугольника со сторонами 1, $\sqrt{2}$ и $\sqrt{3}$, так что

$$(\cos\beta + i\sin\beta) = (1 + \sqrt{-2})/\sqrt{3}.$$

Если бы угол θ был соизмерим с π, то и β был бы соизмерим, поэтому некоторая степень этого комплексного числа равнялась бы единице. Можно проверить, однако, что это не так, поскольку кольцо чисел вида $m + n\sqrt{-2}$ $(m, n \in \mathbb{Z})$ евклидово и разложение на множители в нём однозначно.

Дальнейшее просто: рассмотрим числа π и θ. Они независимы как элементы векторного пространства $\mathbb{R}$ над $\mathbb{Q}$, дополним их до базиса и рассмотрим $\mathbb{Q}$-линейный функционал $\varphi\colon \mathbb{R} \to \mathbb{Q}$, равный коэффициенту при θ в разложении по этому базису. Очевидно, все требования при этом будут выполнены. $\triangleright$

118. Покажите, что некоторое усложнение этого рассуждения позволяет обойтись без базиса Гамеля: достаточно определять φ не на всех действительных числах, а только на линейных комбинациях углов, встречающихся при разрезании куба и тетраэдра на части.

В качестве отступления приведём ещё два странных примера, возникающих благодаря аксиоме выбора (в них даже трансфинитная индукция не используется).

Разноцветные шляпы. Представим себе сначала шеренгу из ста человек в чёрных и белых шляпах. Каждый видит цвета шляп стоящих перед ним, но не видит своей шляпы и шляп позади стоящих, и должен отгадать цвет своей шляпы. Могут ли участники игры договориться заранее, как они должны действовать, чтобы с гарантией большинство догадок было правильными? (Игроки не произносят вслух свои догадки, так что другие игроки не могут их учитывать.)

Легко понять, что стоящая перед игроками задача неразрешима. Стоящий первым в шеренге не видит никого, так что его догадка ни от чего не зависит и заранее предопределена. Наденем ему шляпу другого цвета и сделаем его догадку ошибочной. Цвет шляпы первого определяет догадку второго (у которого нет иной информации), и ему тоже можно надеть шляпу другого цвета. После этого определится догадка третьего, и так далее. Таким образом, для любой стратегии действий игроков есть вариант, в котором все ошибутся.

Ситуация удивительным образом меняется, если игроки стоят в бесконечной шеренге, у которой есть последний, но нет первого, и каждый из игроков видит шляпы впереди стоящих. Другими словами, игроки стоят в точках $0, 1, 2, \ldots$ числовой прямой, глядя вправо, и игрок в точке i знает свою координату и цвета шляп всех следующих игроков $(i+1, i+2, \ldots)$. Его стратегия, таким образом, является функцией, аргумент которой — последовательность цветов видимых им шляп, а значением — догадка о цвете собственной шляпы.

Как ни странно, существуют стратегии игроков, при которых с гарантией все догадки, кроме конечного числа, будут правильными. Чтобы доказать существование таких стратегий, будем называть «раскраской» последовательность цветов шляп всех игроков. Две раскраски будем называть эквивалентными, если они различаются лишь в конечном числе точек (для конечного числа игроков). Выберем в каждом классе эквивалентности по одной «канонической» раскраске. Каждый игрок должен действовать так: видя всех игроков перед собой, он может определить класс эквивалентности раскраски (так как изменение конечного числа остальных игроков, включая его самого́, не меняет этого класса). Затем в качестве догадки он указывает цвет своей шляпы в каноническом представителе этого класса эквивалентности.

Какова бы ни была реальная раскраска, она отличается от эквивалентной ей канонической раскраски лишь в конечном числе мест (по определению эквивалентности). Поэтому все игроки, стоящие дальше этих мест, угадают правильно — у них самих тот же цвет, и видят они то же самое, что в канонической раскраске.

119. Покажите, что игроки могут добиться того же результата (гарантировать конечное число неверных догадок) и в более сложной ситуации, когда они не знают своего положения. (Полезно отдельно рассмотреть классы, содержащие периодические раскраски.)

Неизмеримое множество. Будем считать две точки окружности эквивалентными, если дуга между ними составляет рациональную часть окружности (= измеряется рациональным числом градусов). Это действительно отношение эквивалентности, так как сумма двух рациональных чисел рациональна (транзитивность). Выберем в каждом классе эквивалентности по одной точке; полученное множество «представителей» обозначим M.

Если повернуть множество M на рациональный (в градусах, то есть соизмеримый с окружностью) угол α, то повёрнутое множество M_α не будет пересекаться с исходным: пересечение означало бы, что есть два представителя, отличающихся на α, то есть лежащих в одном и том же классе.

С другой стороны, в объединении множества M_α (при всех рациональных углах поворота α) дают всю окружность (каждая точка имеет представителя в своём классе, и поворот M на соответствующий угол покроет её).

Получается, что окружность разбита на счётное число конгруэнтных (совмещающихся поворотом) множеств. Какую же долю окруж-

ности (по мере) составляет каждое множество? Поскольку множества конгруэнтны, то эти доли равны; поскольку они все помещаются в окружности без пересечений, то доля не может быть положительной, то есть равна нулю.

Как ни странно, в объединении счётное число таких «нулевых» множеств составляет всю окружность. (Говоря более формально, не существует ненулевой счётно-аддитивной меры, определённой на всех подмножествах окружности и инвариантной относительно поворотов.)

Ещё удивительнее пространственный вариант этого примера: можно разбить шар на конечное число непересекающихся множеств, из которых (сдвинув каждую часть в пространстве) можно получить два шара того же размера. Этот пример называют «парадоксом Банаха – Тарского». Но это построение сложнее и требует знакомства с алгеброй (в одном из вариантов используется свободная подгруппа с двумя образующими в группе $SO(3)$).

2.8. Лемма Цорна и её применения

В современных учебниках редко встречается трансфинитная индукция как таковая: она заменяется ссылкой на так называемую лемму Цорна. Сейчас мы покажем, как это делается, на примере теоремы о существовании базиса в линейном пространстве.

Теорема 30 (лемма Цорна). Пусть Z — частично упорядоченное множество, в котором всякая цепь имеет верхнюю границу. Тогда в этом множестве есть максимальный элемент, и, более того, для любого элемента $a \in Z$ существует элемент $b \geqslant a$, являющийся максимальным в Z. (*Цепь* — это подмножество, любые два элемента которого сравнимы. Верхняя граница цепи — элемент, больший или равный любого элемента цепи.)

$\lhd$ Прежде всего отметим, что Z лишь частично упорядочено, поэтому надо различать максимальные и наибольшие элементы. По этой же причине мы вынуждены употреблять грамматически некорректную конструкцию «больший или равный любого (любому?)», поскольку сказать «не меньше любого» (стандартный выход из положения) означало бы изменить смысл.

Доказательство повторяет рассуждения при построении базиса, но в более общей ситуации (теперь у нас не линейно независимые семейства, а произвольные элементы Z).

Пусть дан произвольный элемент a. Предположим, что не суще-

ствует максимального элемента, большего или равного a. Это значит, что для любого $b \geqslant a$ найдётся $c > b$. Тогда $c > a$ и потому найдётся $d > c$ и т. д. Продолжая этот процесс достаточно долго, мы исчерпаем все элементы Z и придём к противоречию.

Проведём рассуждение аккуратно (пока что мы даже не использовали условие леммы, касающееся цепей). Возьмём вполне упорядоченное множество I достаточно большой мощности (большей, чем мощность Z). Построим строго возрастающую функцию $f\colon I \to Z$ по трансфинитной рекурсии. Её значение на минимальном элементе I будет равно a. Предположим, что мы уже знаем все её значения на всех элементах, меньших некоторого i. В силу монотонности эти значения попарно сравнимы. Поэтому существует их верхняя граница s, которая, в частности, больше или равна a. Возьмём какой-то элемент $t > s$ и положим $f(i) = t$; по построению монотонность сохранится. Тем самым I равномощно части Z, что противоречит его выбору.

В этом рассуждении, формально говоря, есть пробел: мы одновременно определяем функцию по трансфинитной рекурсии и доказываем её монотонность с помощью трансфинитной индукции. Наше рекурсивное определение имеет смысл, лишь если уже построенная часть функции монотонна. Формально говоря, надо воспользоваться теоремой 19, считая, что следующее значение не определено, если уже построенный участок не монотонен, и получить функцию, определённую на всём I или на начальном отрезке. Если она определена на некотором начальном отрезке, то она монотонна на нём по построению, поэтому следующее значение тоже определено — противоречие. $\triangleright$

Как и при построении базиса Гамеля (задача 115, с. 70), можно обойтись без множества большей мощности. Вполне упорядочим множество Z с помощью теоремы Цермело. Этот порядок никак не связан с исходным порядком на Z; мы будем обозначать его символом $\prec$. Построим с помощью трансфинитной рекурсии функцию $f\colon Z \to Z$ с такими свойствами: (1) $f(z) \geqslant a$ для любого $z \in Z$; (2) f монотонна в следующем смысле: если $x \prec y$, то $f(x) \leqslant f(y)$; (3) $f(z)$ не может быть строго меньше z (в смысле исходного порядка $\leqslant$) ни при каком z.

Делается это так. Значение $f(z_0)$ для $\prec$-наименьшего элемента z_0 мы положим равным либо a, либо z_0 (последнее — если $z_0 > a$). Значение $f(z)$ для остальных z есть либо верхняя граница значений $f(z')$ при $z' \prec z$ (по предположению индукции множество таких

значений линейно упорядочено и потому имеет некоторую верхнюю границу α), либо само z (последнее — если $z > \alpha$).

В силу монотонности множество значений функции f линейно упорядочено и имеет верхнюю границу. Эта граница (обозначим её β) больше или равна a (которое есть $f(z_0)$) и является искомым максимальным элементом: если $\beta < z$ для некоторого z, то $f(z) \leqslant \beta < z$, что противоречит свойству (3).

120. Проведите это рассуждение подробно.

Теперь повторим доказательство теоремы о базисе, используя лемму Цорна. Пусть V — произвольное векторное пространство. Рассмотрим частично упорядоченное множество Z, состоящее из линейно независимых подмножеств пространства V. Порядок на Z задаётся отношением «быть подмножеством».

Проверим, что условия леммы выполнены. Пусть имеется некоторая цепь, то есть семейство линейно независимых множеств, причём любые два множества этого семейства сравнимы. Объединим все эти множества и покажем, что полученное множество будет линейно независимым (тем самым оно будет верхней границей элементов цепи). В самом деле, нетривиальная линейная комбинация включает в себя какое-то конечное число векторов, каждый из своего множества. Этих множеств конечное число, и потому среди них есть наибольшее по включению (в конечном линейно упорядоченном множестве есть наибольший элемент). Это наибольшее множество содержит все векторы нетривиальной линейной комбинации, и линейно независимо по предположению, так что наша нетривиальная линейная комбинация отлична от нуля.

Таким образом, можно применить лемму Цорна и заключить, что любое линейно независимое множество векторов содержится в максимальном линейно независимом множестве векторов. К нему уже нельзя добавить ни одного вектора, не создав линейной зависимости, и оно является искомым базисом.

Аналогичным образом можно доказать существование ортогонального базиса в гильбертовом пространстве (там определение базиса другое: разрешаются бесконечные линейные комбинации, понимаемые как суммы рядов) или существование базиса трансцендентности (максимальная алгебраически независимая система элементов в расширении полей).

Мы приведём другой пример применения леммы Цорна, где фигурируют уже известные нам понятия.

Теорема 31. Всякий частичный порядок может быть продолжен до линейного.

$\triangleleft$ Пусть $(X, \leqslant)$ — частично упорядоченное множество. Теорема утверждает, что существует отношение порядка $\leqslant'$ на X, продолжающее исходное (это значит, что $x \leqslant y \Rightarrow x \leqslant' y$) и являющееся отношением линейного порядка. (Кстати, отметим, что слово «линейного» в формулировке теоремы нельзя заменить на слово «полного» — например, если исходный порядок линейный, но не полный.)

Готовясь к применению леммы Цорна, рассмотрим частично упорядоченное множество Z, элементами которого будут частичные порядки на X (то есть подмножества множества $X \times X$, обладающие свойствами рефлексивности, транзитивности и антисимметричности), упорядоченные по включению: $\leqslant_1$ считается меньшим или равным $\leqslant_2$, если $\leqslant_2$ продолжает $\leqslant_1$ (из $x \leqslant_1 y$ следует $x \leqslant_2 y$).

Легко проверить, что условие леммы Цорна выполнено: если у нас есть семейство частичных порядков, линейно упорядоченное по включению, то объединение этих порядков является частичным порядком, и этот порядок будет верхней границей семейства. (Проверим, например, что объединение обладает свойством транзитивности. Пусть $x \leqslant_1 y$ в одном из порядков семейства ($\leqslant_1$), а $y \leqslant_2 z$ в другом; один из порядков (например, $\leqslant_1$) продолжает другой, тогда $x \leqslant_1 y \leqslant_1 z$ и потому $x \leqslant z$ в объединении. Рефлексивность и антисимметричность проверяются столь же просто.)

Следовательно, по лемме Цорна на множестве X существует максимальный частичный порядок, продолжающий исходный. Обозначим его как $\leqslant$ (путаницы с исходным порядком не возникнет, так как исходный нам больше не нужен). Нам надо показать, что он будет линейным. Пусть $x, y \in X$ — два несравнимых элемента. Расширим порядок до нового порядка $\leqslant'$, при котором $x \leqslant' y$. Этот новый порядок определяется так: $a \leqslant' b$, если (1) $a \leqslant b$ или (2) $a \leqslant x$ и $y \leqslant b$. Несложно проверить, что $\leqslant'$ будет частичным порядком. Рефлексивность очевидна. Транзитивность: если $a \leqslant' b$ и $b \leqslant' c$, то есть четыре возможности. Если в обоих случаях имеет место случай (1), то $a \leqslant \leqslant b \leqslant c$ и всё очевидно. Если $a \leqslant' b$ в силу (1), а $b \leqslant c$ в силу (2), то $a \leqslant b \leqslant x$ и $y \leqslant c$, так что $a \leqslant' c$ в силу (2). Аналогично рассматривается и симметричный случай. Наконец, двукратная ссылка на (2) невозможна, так как тогда $(a \leqslant x)$, $(y \leqslant b)$, $(b \leqslant x)$ и $(y \leqslant c)$, и получается, что $y \leqslant b \leqslant x$, а мы предполагали, что x и y не сравнимы. Антисимметричность доказывается аналогично. Таким образом, отношение $\leqslant'$ будет частичным порядком, строго содержащим $\leqslant$, что

противоречит максимальности. ▷

121. Покажите, что любое бинарное отношение без циклов (цикл образуется, если xRx, или $xRyRx$, или $xRyRzRx$ и т. д.) может быть продолжено до линейного порядка. (Для конечных множеств поиск такого продолжения обычно называют «топологической сортировкой».)

122. Множество на плоскости называется *выпуклым*, если вместе с любыми двумя точками оно содержит соединяющий их отрезок. Покажите, что любые два непересекающихся выпуклых множества можно разделить прямой (каждое множество лежит по одну сторону от прямой, возможно, пересекаясь с ней). (Указание. Используя лемму Цорна, можно расширить исходные непересекающиеся множества A и B до взаимно дополнительных выпуклых множеств A' и B'. Затем можно убедиться, что граница между A' и B' представляет собой прямую.)

123. Покажите, что все подмножества натурального ряда можно разбить на «большие» и «малые» таким образом, чтобы выполнялись следующие свойства: (1) множество большое тогда и только тогда, когда его дополнение мало; (2) любое подмножество малого множества мало, а любое надмножество большого множества — большое; (3) объединение двух малых множеств мало, а пересечение двух больших множеств — большое; (4) все конечные множества — малые, а все множества с конечными дополнениями — большие. (Вначале будем требовать условий (1) – (4), но не настаивать на том, что любое множество должно быть большим или малым. Например, можно считать малыми конечные множества, а большими — их дополнения. Затем можно добавлять множества, определяя их в большие или малые, применив трансфинитную индукцию или лемму Цорна.)

Построенное в этой задаче деление множеств на большие и малые (точнее, класс больших множеств) называют *неглавным ультрафильтром*; слово «ультра» здесь соответствует требованию того, что всякое множество большое или малое; слово «неглавный» обозначает требование (4).

124. (Продолжение.) Два агрессора играют в такую игру: сначала первый захватывает начальный отрезок натурального ряда произвольного размера (от 0 до какого-то k), затем второй захватывает примыкающий отрезок (от $k+1$ до какого-то l, затем первый захватывает следующий (от $l+1$ до какого-то m), и т. д. Игра бесконечна; победителем в бесконечной партии считается тот игрок, который захватил большое множество. Покажите, что в этой игре ни один из игроков не имеет выигрышной стратегии. (Выигрышную стратегию для одного мог бы использовать и другой, поскольку конечный начальный участок не влияет на исход игры.)

2.9. Свойства операций над мощностями

Теперь мы можем доказать несколько утверждений о мощностях.

Теорема 32. Если A бесконечно, то множество $A \times \mathbb{N}$ равномощно A.

$\lhd$ Вполне упорядочим множество A. Мы уже знаем (см. с. 56), что всякий элемент множества A однозначно представляется в виде $z+n$, где z — предельный элемент (не имеющий непосредственно предыдущего), а n — натуральное число. Это означает, что A равномощно $B \times \mathbb{N}$, где B — множество предельных элементов. (Тут есть небольшая трудность — последняя группа элементов конечна, если в множестве есть наибольший элемент. Но мы уже знаем, что добавление конечного или счётного множества не меняет мощности, так что этим можно пренебречь.)

Теперь утверждение теоремы очевидно: $A \times \mathbb{N}$ равномощно $(B \times \mathbb{N}) \times \mathbb{N}$, то есть $B \times (\mathbb{N} \times \mathbb{N})$ и тем самым $B \times \mathbb{N}$ (произведение счётных множеств счётно), то есть A. $\rhd$

По теореме Кантора – Бернштейна отсюда следует, что промежуточные мощности (в частности, $|A| + |A|$, а также любое произведение A и конечного множества) совпадают с $|A|$. Ещё одно следствие полезно выделить:

Теорема 33. Сумма двух бесконечных мощностей равна их максимуму.

$\lhd$ Прежде всего напомним, что любые две мощности сравнимы (теорема 25, с. 68). Пусть, скажем, $|A| \leqslant |B|$. Тогда $|B| \leqslant |A| + |B| \leqslant |B| + |B| \leqslant |B| \times \aleph_0 = |B|$ (последнее неравенство — утверждение предыдущей теоремы). Остаётся воспользоваться теоремой Кантора – Бернштейна и заключить, что $|B| = |A + B|$. $\rhd$

Теперь можно доказать более сильное утверждение.

Теорема 34. Если A бесконечно, то $A \times A$ равномощно A.

$\lhd$ Заметим, что для счётного множества (как, впрочем, и для континуума — но это сейчас не важно) мы это уже знаем. Поэтому в A есть подмножество, равномощное своему квадрату.

Рассмотрим семейство всех таких подмножеств вместе с соответствующими биекциями. Элементами этого семейства будут пары $\langle B, f \rangle$, где B — подмножество A, а $f\colon B \to B \times B$ — взаимно однозначное соответствие. Введём на этом семействе частичный порядок: $\langle B_1, f_1 \rangle \leqslant \langle B_2, f_2 \rangle$, если $B_1 \subset B_2$ и ограничение отображения f_2 на B_1 совпадает с f_1 (рис. 6).

Теперь применим лемму Цорна. Для этого нужно убедиться, что

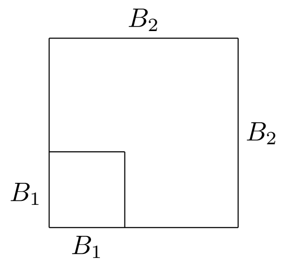


Рис. 6. Отображение f_1 — взаимно однозначное соответствие между малым квадратом и его стороной; f_2 добавляет к нему взаимно однозначное соответствие между $B_2 \setminus B_1$ и «уголком» $(B_2 \times B_2) \setminus (B_1 \times B_1)$.

любое линейно упорядоченное (в смысле описанного порядка) множество пар указанного вида имеет верхнюю границу. В самом деле, объединим все первые компоненты этих пар; пусть B — их объединение. Как обычно, согласованность отображений (гарантируемая определением порядка) позволяет соединить отображения в одно. Это отображение (назовём его f) отображает B в $B \times B$. Оно будет инъекцией: значения $f(b')$ и $f(b'')$ при различных b' и b'' различны (возьмём большее из множеств, которым принадлежат b' и b''; на нём f является инъекцией по предположению). С другой стороны, f является сюръекцией: для любой пары $\langle b', b'' \rangle \in B \times B$ возьмём множества, из которых произошли b' и b'', выберем из них большее и вспомним, что мы имели взаимно однозначное соответствие между ним и его квадратом.

По лемме Цорна в нашем частично упорядоченном множестве существует максимальный элемент. Пусть этот элемент есть $\langle B, f \rangle$. Мы знаем, что f есть взаимно однозначное соответствие между B и $B \times B$ и потому $|B| = |B| \times |B|$. Теперь есть две возможности. Если B равномощно A, то $B \times B$ равномощно $A \times A$ и всё доказано. Осталось рассмотреть случай, когда B не равномощно A, то есть имеет меньшую мощность (большей оно иметь не может, будучи подмножеством). Пусть C — оставшаяся часть A, то есть $A \setminus B$. Тогда $|A| = |B| + |C| = \max(|B|, |C|)$, следовательно, C равномощно A и больше B по мощности. Возьмём в C часть C', равномощную B, и положим $B' = B + C'$ (рис. 7). Обе части множества B' равномощны B. Поэтому $B' \times B'$ разбивается на 4 части, каждая из которых равномощна $B \times B$, и, следовательно, равномощна B (напомним, что

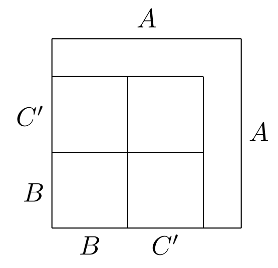


Рис. 7. Продолжение соответствия с B на $B' = B + C'$.

у нас есть взаимно однозначное соответствие f между B и $B \times B$). Соответствие f можно продолжить до соответствия f' между B' и $B' \times B'$, дополнив его соответствием между C' и $(B' \times B') \setminus (B \times B)$ (эта разность состоит из трёх множеств, равномощных B, так что равномощна B). В итоге мы получаем бо́льшую пару $\langle B', f' \rangle$, что противоречит утверждению леммы Цорна о максимальности. Таким образом, этот случай невозможен. $\triangleright$

Выведем теперь некоторые следствия из доказанного утверждения.

Теорема 35. (а) Произведение двух бесконечных мощностей равно большей из них. (б) Если множество A бесконечно, то множество A^n всех последовательностей длины $n > 0$, составленных из элементов A, равномощно A. (в) Если множество A бесконечно, то множество всех конечных последовательностей, составленных из элементов A, равномощно A.

$\triangleleft$ Первое утверждение доказывается просто: если $|A| \leqslant |B|$, то $|B| \leqslant |A| \times |B| \leqslant |B| \times |B| = |B|$.

Второе утверждение легко доказывается индукцией по n: если $|A^n| = |A|$, то $|A^{n+1}| = |A^n| \times |A| = |A| \times |A| = |A|$.

Третье тоже просто: множество конечных последовательностей есть $1 + A + A^2 + A^3 + \ldots$; каждая из частей (кроме первой, которой можно пренебречь) равномощна A (по доказанному), и потому всё вместе есть $|A| \times \aleph_0 = |A|$. $\triangleright$

Заметим, что из последнего утверждения теоремы вытекает, что семейство всех конечных подмножеств бесконечного множества A имеет ту же мощность, что и A (подмножеств не больше, чем конечных последовательностей и не меньше, чем одноэлементных подмножеств).

125. Пусть A бесконечно. Докажите, что $|A^A| = |2^A|$.

126. Рассмотрим мощность $\alpha = \aleph_0 + 2^{\aleph_0} + 2^{(2^{\aleph_0})} + \ldots$ (счётная сумма). Покажите, что α — минимальная мощность, которая больше мощностей множеств $\mathbb{N}$, $P(\mathbb{N})$, $P(P(\mathbb{N}))$, ... Покажите, что $\alpha^{\aleph_0} = 2^\alpha > \alpha$.

Теперь мы можем доказать упоминавшееся ранее утверждение о равномощности базисов.

Теорема 36. Любые два базиса в бесконечномерном векторном пространстве имеют одинаковую мощность.

$\triangleleft$ Пусть даны два базиса — первый и второй. Для каждого вектора из первого базиса фиксируем какой-либо способ выразить его через векторы второго базиса. В этом выражении участвует конечное множество векторов второго базиса. Таким образом, есть некоторая функция, которая каждому вектору первого базиса ставит в соответствие некоторое конечное множество векторов второго. Как мы только что видели, возможных значений этой функции столько же, сколько элементов во втором базисе. Кроме того, прообраз каждого значения состоит из векторов первого базиса, выражающихся через данный (конечный) набор векторов второго, и потому конечен. Выходит, что первый базис разбит на группы, каждая группа конечна, а всего групп не больше, чем векторов во втором базисе. Поэтому мощность первого базиса не превосходит мощности второго, умноженной на $\aleph_0$ (от чего, как мы знаем, мощность бесконечного множества не меняется). Осталось провести симметричное рассуждение и сослаться на теорему Кантора–Бернштейна. $\triangleright$

2.10. Ординалы

Как мы уже говорили, *ординалом* называется порядковый тип вполне упорядоченного множества, то есть класс всех изоморфных ему упорядоченных множеств (естественно, они будут вполне упорядоченными).

На ординалах естественно определяется линейный порядок. Чтобы сравнить два ординала α и β, возьмём их представители A и B. Применим теорему 22 и посмотрим, какой из трёх случаев (A изоморфно начальному отрезку B, отличному от всего B; множества A и B изоморфны; B изоморфно начальному отрезку A, отличному от всего A) имеет место. В первом случае $\alpha < \beta$, во втором $\alpha = \beta$, в третьем $\alpha > \beta$.

Мы отвлекаемся от трудностей, связанных с основаниями теории множеств (см. раздел 1.6); как формально можно оправдать наши рассуждения, мы ещё обсудим. Пока что отметим некоторые свойства ординалов.

- Мы определили на ординалах линейный порядок. Этот порядок будет полным: любое непустое семейство ординалов имеет наименьший элемент (теорема 23; разница лишь в том, что мы не употребляли там слова «ординал», а говорили о представителях).

- Пусть α — некоторый ординал. Рассмотрим начальный отрезок $[0, \alpha)$ в классе ординалов (образованный всеми ординалами, меньшими α в смысле указанного порядка). Этот отрезок упорядочен по типу α (то есть изоморфен представителям ординала α). В самом деле, пусть A — один из представителей ординала α. Ординалы, меньшие α, соответствуют собственным (не совпадающим с A) начальным отрезкам множества A. Такие отрезки имеют вид $[0, a)$ и тем самым находятся во взаимно однозначном соответствии с элементами множества A. (Легко проверить, что это соответствие сохраняет порядок.)

  Сказанное можно переформулировать так: каждый ординал упорядочен как множество меньших ординалов. (В одном из формальных построений теории ординалов каждый ординал *равен* множеству всех меньших ординалов.)

- Ординал называется *непредельным*, если существует непосредственно предшествующий ему (в смысле указанного порядка) ординал. Если такого нет, ординал называют *предельным*.

- Любое ограниченное семейство ординалов имеет точную верхнюю грань (наименьший ординал, больший или равный всем ординалам семейства). В самом деле, возьмём какой-то ординал β, являющийся верхней границей. Тогда все ординалы семейства изоморфны начальным отрезкам множества B, представляющего ординал β. Если среди этих отрезков есть само B, то β будет точной верхней гранью (и наибольшим элементом семейства). Если нет, то эти отрезки имеют вид $[0, b)$ для различных элементов $b \in B$. Рассмотрим множество S всех таких элементов b. Если S не ограничено в B, то β будет точной верхней гранью. Если S ограничено, то оно имеет точную верхнюю грань s, и $[0, s)$ будет точной верхней гранью семейства.

Можно сказать, что семейство ординалов — это как бы универсальное вполне упорядоченное семейство; любое вполне упорядоченное множество изоморфно некоторому начальному отрезку этого се-

мейства. Поэтому мы немедленно придём к противоречию, если захотим рассмотреть множество всех ординалов (ведь для всякого вполне упорядоченного множества есть ещё большее — добавим к нему новый элемент, больший всех предыдущих). Этот парадокс называется *парадоксом Бурали-Форти*.

127. Докажите, что точная верхняя грань счётного числа счётных ординалов счётна.

Как же рассуждать об ординалах, не впадая в противоречия? В принципе можно заменять утверждения об ординалах утверждениями о их представителях и воспринимать упоминания ординалов как «вольность речи». Другой подход (предложенный фон Нейманом) применяется при аксиоматическом построении теории множеств, и состоит он примерно в следующем: мы объявляем каждый ординал равным множеству всех меньших ординалов. Тогда минимальный ординал 0 (порядковый тип пустого множества) будет пустым множеством $\varnothing$, следующий за ним ординал 1 (порядковый тип одноэлементного множества) будет $\{0\} = \{\varnothing\}$, затем $2 = \{0, 1\} = \{\varnothing, \{\varnothing\}\}$, $3 = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, $4 = \{0, 1, 2, 3\}$ и т. д. За ними следует ординал ω (порядковый тип множества натуральных чисел), равный $\{0, 1, 2, 3, \ldots\}$, потом $\omega + 1 = \{0, 1, 2, 3, \ldots, \omega\}$, потом $\omega + 2 = \{0, 1, 2, 3, \ldots, \omega, \omega + 1\}$ и т. д.

Мы не будем говорить подробно об аксиоматической теории множеств Цермело – Френкеля, но два обстоятельства следует иметь в виду. Во-первых, в ней нет никаких объектов, кроме множеств, и есть *аксиома экстенсиональности* (или *объёмности*), которая говорит, что два объекта, содержащие одни и те же элементы, равны. Поэтому существует лишь один объект, не содержащий элементов (пустое множество). Во-вторых, в ней есть *аксиома фундирования*, которая говорит, что отношение $\in$ фундировано: во всяком множестве X есть элемент, являющийся $\in$-минимальным, то есть элемент $x \in X$, для которого $X \cap x = \varnothing$. Отсюда следует, что никакое множество x не может быть своим элементом (иначе для множества $\{x\}$ нарушалась бы аксиома фундирования).

128. Выведите из аксиомы фундирования, что не существует множеств x, y, z, для которых $x \in y \in z \in x$.

Философски настроенный математик обосновал бы аксиому фундирования так: множества строятся из ранее построенных множеств, начиная с пустого, и поэтому возможна индукция по построению (доказывая какое-либо свойство множеств, можно рассуждать индуктивно и предполагать, что оно верно для всех его элементов).

Теперь можно определить ординалы так. Будем говорить, что множество x *транзитивно*, если всякий элемент множества x является подмножеством множества x, то есть если из $z \in y \in x$ следует $z \in x$. Назовём *ординалом* транзитивное множество, всякий элемент которого транзитивен. Это требование гарантирует, что на элементах любого ординала отношение $\in$ является (строгим) частичным порядком.

Аксиома фундирования гарантирует, что частичный порядок $\in$ на любом ординале является фундированным. После этого по индукции можно доказать, что он является линейным (и, следовательно, полным).

129. (**а**) Используя определение ординала как транзитивного множества с транзитивными элементами, докажите, что элемент ординала есть ординал. (**б**) Пусть α — ординал (в смысле данного нами определения). Докажите, что отношение $\in$ на нём является частичным порядком. (**в**) Докажите, что для любых элементов $a, b \in \alpha$ верно ровно одно из трёх соотношений: либо $a \in b$, либо $a = b$, либо $b \in a$. (Указание: используйте двойную индукцию по фундированному отношению $\in$ на α, а также аксиому экстенсиональности.) (**г**) Докажите, что один ординал изоморфен собственному начальному отрезку другого тогда и только тогда, когда является его элементом. (Таким образом, отношение $<$ на ординалах как упорядоченных множествах совпадает с отношением принадлежности.) Докажите, что каждый ординал является множеством всех меньших его ординалов.

Заметим ещё, что если каждый ординал есть множество всех меньших его ординалов, то точная верхняя грань множества ординалов есть их объединение.

Мы не будем подробно развивать этот подход и по-прежнему будем наивно представлять себе ординалы как порядковые типы вполне упорядоченных множеств.

Прежде чем перейти к сложению и умножению ординалов, отметим такое свойство:

Теорема 37. Пусть A — подмножество вполне упорядоченного множества B. Тогда порядковый тип множества A не превосходит порядкового типа множества B.

$\triangleleft$ Отметим сразу же, что равенство возможно, даже если A является собственным подмножеством B. Например, чётные натуральные числа имеют тот же порядковый тип ω, что и все натуральные числа.

Рассуждая от противного, предположим, что порядковый тип

множества A больше. Тогда B изоморфно некоторому начальному отрезку множества A, не совпадающему со всем A. Пусть a_0 — верхняя граница (в A) этого отрезка, а $f: B \to A$ — соответствующий изоморфизм. Тогда f строго возрастает и потому $f(b) \geqslant b$ для всех $b \in B$ (теорема 17). В частности, $f(a_0) \geqslant a_0$, но по предположению любое значение $f(b)$ меньше a_0 — противоречие. $\triangleright$

2.11. Арифметика ординалов

Мы определили сумму и произведение линейно упорядоченных множеств в разделе 2.1. (Напомним, что в $A + B$ элементы A предшествуют элементам B, а в $A \times B$ мы сначала сравниваем B-компоненты пар, а в случае их равенства — A-компоненты.)

Легко проверить следующие свойства сложения:

- Сложение ассоциативно: $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
- Сложение не коммутативно: например, $1 + \omega = \omega$, но $\omega + 1 \neq \omega$.
- Очевидно, $\alpha + 0 = 0 + \alpha = \alpha$.
- Сумма возрастает при росте второго аргумента: если $\beta_1 < \beta_2$, то $\alpha + \beta_1 < \alpha + \beta_2$. (В самом деле, пусть β_1 изоморфно начальному отрезку в β_2, отличному от всего β_2. Добавим к этому изоморфизму тождественное отображение на α и получим изоморфизм между $\alpha + \beta_1$ и начальным отрезком в $\alpha + \beta_2$, отличным от $\alpha + \beta_2$.)
- Сумма неубывает при росте первого аргумента: если $\alpha_1 < \alpha_2$, то $\alpha_1 + \beta \leqslant \alpha_2 + \beta$. (В самом деле, $\alpha_1 + \beta$ изоморфно подмножеству в $\alpha_2 + \beta$. Это подмножество не является начальным отрезком, но мы можем воспользоваться теоремой 37.)
- Определение суммы согласовано с обозначением $\alpha + 1$ для следующего за α ординала. (Здесь 1 — порядковый тип одноэлементного множества.) Следующим за $\alpha + 1$ ординалом будет ординал $(\alpha + 1) + 1 = \alpha + (1 + 1) = \alpha + 2$ и т. д.
- Если $\alpha \geqslant \beta$, то существует единственный ординал γ, для которого $\beta + \gamma = \alpha$. (В самом деле, β изоморфно начальному отрезку в α; оставшаяся часть α и будет искомым ординалом γ. Единственность следует из монотонности сложения по второму аргументу.) Заметим, что эту операцию можно называть «вычитанием слева».

- «Вычитание справа», напротив, возможно не всегда. Пусть α — некоторый ординал. Тогда уравнение $\beta + 1 = \alpha$ (относительно β) имеет решение тогда и только тогда, когда α — непредельный ординал, (т. е. когда α имеет наибольший элемент).

Определение суммы двух ординалов в силу ассоциативности можно распространить на любое конечное число ординалов. Можно определить и сумму $\alpha_1 + \alpha_2 + \ldots$ счётной последовательности ординалов (элементы α_i предшествуют элементам α_j при $i < j$; внутри каждого α_i порядок прежний). Как легко проверить, это множество действительно будет вполне упорядоченным: чтобы найти минимальный элемент в его подмножестве, рассмотрим компоненты, которые это подмножество задевает, выберем из них компоненту с наименьшим номером и воспользуемся её полной упорядоченностью.

В этом построении можно заменить натуральные числа на элементы произвольного вполне упорядоченного множества I и определить сумму $\sum A_i$ семейства вполне упорядоченных множеств A_i, индексированного элементами I, как порядковый тип множества всех пар вида $\langle a, i\rangle$, для которых $a \in A_i$. При сравнении пар сравниваются вторые компоненты, а в случае равенства и первые (в соответствующем A_i). Если все A_i изоморфны одному и тому же множеству A, получаем уже известное нам определение произведения $A \times I$.

Теперь перейдём к умножению ординалов.

- Умножение ассоциативно: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. (В самом деле, в обоих случаях по существу получается множество троек; тройки сравниваются справа налево, пока не обнаружится различие.)

- Умножение не коммутативно: например, $2 \cdot \omega = \omega$, в то время как $\omega \cdot 2 \neq \omega$.

- Очевидно, $\alpha \cdot 0 = 0 \cdot \alpha = 0$ и $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$.

- Выполняется одно из свойств дистрибутивности: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (непосредственно следует из определения). Симметричное свойство выполнено не всегда: $(1 + 1) \cdot \omega = \omega \neq \omega + \omega$.

- Произведение строго возрастает при увеличении второго множителя, если первый не равен 0. (Для разнообразия выведем это из ранее доказанных свойств: если $\beta_2 > \beta_1$, то $\beta_2 = \beta_1 + \delta$, так что $\alpha\beta_2 = \alpha(\beta_1 + \delta) = \alpha\beta_1 + \alpha\delta > \alpha\beta_1$.)

- Произведение не убывает при возрастании первого множителя. (В самом деле, если $\alpha_1 < \alpha_2$, то $\alpha_1\beta$ изоморфно подмножеству $\alpha_2\beta$. Это подмножество не является начальным отрезком, но можно сослаться на теорему 37.)

- Любой ординал, меньший $\alpha\beta$, однозначно представим в виде $\alpha\beta' + \alpha'$, где $\beta' < \beta$ и $\alpha' < \alpha$.

  (В самом деле, пусть множества A и B упорядочены по типам α и β. Тогда $A \times B$ упорядочено по типу $\alpha\beta$. Всякий ординал, меньший $\alpha\beta$, есть начальный отрезок в $A \times B$, ограниченный некоторым элементом $\langle a, b\rangle$. Начальный отрезок $[0, \langle a, b\rangle)$ состоит из пар, у которых второй член меньше b, а также из пар, у которых второй член равен b, а первый меньше a. Отсюда следует, что этот начальный отрезок изоморфен $A \times [0, b) + [0, a)$, так что остаётся положить $\beta' = [0, b)$ и $\alpha' = [0, a)$. Теперь проверим однозначность. Пусть $\alpha\beta' + \alpha' = \alpha\beta'' + \alpha''$. Если $\beta' = \beta''$, то можно воспользоваться однозначностью левого вычитания и получить, что $\alpha' = \alpha''$. Остаётся проверить, что β' не может быть, скажем, меньше β''. В этом случае $\beta'' = \beta' + \delta$, и сокращая $\alpha\beta'$ слева, получим, что $\alpha' = \alpha\delta + \alpha''$, что невозможно, так как левая часть меньше α, а правая часть больше или равна α.)

- Аналогичное «деление с остатком» возможно и для любых ординалов. Пусть $\alpha > 0$. Тогда любой ординал γ можно разделить с остатком на α, то есть представить в виде $\alpha\tau + \rho$, где $\rho < \alpha$, и притом единственным образом.

  (В самом деле, существование следует из предыдущего утверждения, надо только взять достаточно большое β, чтобы $\alpha\beta$ было больше γ, скажем, $\beta = \gamma + 1$. Единственность доказывается так же, как и в предыдущем пункте.)

- Повторяя деление с остатком на $\alpha > 0$, можно построить позиционную систему счисления для ординалов: всякий ординал, меньший α^{k+1} (здесь k — натуральное число), можно однозначно представить в виде $\alpha^k\beta_k + \alpha^{k-1}\beta_{k-1} + \ldots + \alpha\beta_1 + \beta_0$, где «цифры» $\beta_k, \ldots, \beta_1, \beta_0$ — ординалы, меньшие α.

130. Для каких ординалов $1 + \alpha = \alpha$?
131. Для каких ординалов $2 \cdot \alpha = \alpha$?
132. Какие ординалы представимы в виде $\omega \cdot \alpha$?

133. Докажите, что $\alpha + \beta = \beta$ тогда и только тогда, когда $\alpha\omega \leqslant \beta$ (здесь α и β — ординалы).

134. Докажите, что если $\alpha + \beta = \beta + \alpha$ для некоторых ординалов α и β, то найдётся такой ординал γ и такие натуральные числа m и n, что $\alpha = \gamma m$ и $\beta = \gamma n$.

135. Определим операцию «замены основания» с $k > 1$ на $l > k$. Чтобы применить эту операцию к натуральному числу n, надо записать n в k-ичной системе счисления, а затем прочесть эту запись в l-ичной системе. (Очевидно, число при этом возрастёт, если оно было больше или равно k.) Возьмём произвольное число n и будет выполнять над ним такие операции: замена основания с 2 на 3 – вычитание единицы – замена основания с 3 на 4 – вычитание единицы – замена основания с 4 на 5 – вычитание единицы – …Докажите, что рано или поздно мы получим нуль и вычесть единицу не удастся. (Указание: замените все основания на ординал ω; получится убывающая последовательность ординалов.)

2.12. Индуктивные определения и степени

Мы определили сложение и умножение ординалов с помощью явных конструкций порядка на соответствующих множествах. Вместо этого можно было бы их определить индуктивно.

Теорема 38. Сложение ординалов обладает следующими свойствами:

$$\begin{aligned} \alpha + 0 &= \alpha; \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1; \\ \alpha + \gamma &= \sup\{\alpha + \beta \mid \beta < \gamma\} \text{ для предельного } \gamma \neq 0. \end{aligned}$$

Эти свойства однозначно определяют операцию сложения.

$\lhd$ Два первых свойства очевидны; проверим третье. Если $\beta < \gamma$, то $\alpha + \beta < \alpha + \gamma$, так что $\alpha + \gamma$ будет верхней границей всех сумм вида $\alpha + \beta$ при $\beta < \gamma$. Надо проверить, что эта граница точная. Пусть некоторый ординал τ меньше $\alpha + \gamma$. Убедимся, что он меньше $\alpha + \beta$ для некоторого $\beta < \gamma$. Если $\tau < \alpha$, всё очевидно. Если $\tau \geqslant \alpha$, представим его в виде $\tau = \alpha + \sigma$. Тогда $\alpha + \sigma < \alpha + \gamma$ и потому $\sigma < \gamma$. Поскольку ординал γ предельный, $\sigma + 1$ также меньше γ и остаётся положить $\beta = \sigma + 1$.

Указанные свойства однозначно определяют операцию сложения, так как представляют собой рекурсивное определение по β (если есть две операции сложения, обладающие этими свойствами, возьмём минимальное β, для которого они различаются и т. д.). $\rhd$

Аналогично можно определить и умножение:

Теорема 39. Умножение ординалов обладает следующими свойствами:

$$\alpha 0 = 0;$$
$$\alpha(\beta + 1) = \alpha\beta + \alpha;$$
$$\alpha\gamma = \sup\{\alpha\beta \mid \beta < \gamma\} \text{ для предельного } \gamma \neq 0.$$

Эти свойства однозначно определяют операцию умножения.

$\triangleleft$ Доказательство аналогично, нужно только проверить, что если $\tau < \alpha\gamma$ для предельного γ, то $\tau < \alpha\beta$ для некоторого $\beta < \gamma$. Как мы видели на с. 89, ординал τ имеет вид $\tau = \alpha\gamma' + \alpha'$ при $\gamma' < \gamma$; достаточно положить $\beta = \gamma' + 1$. $\triangleright$

Возникает естественное желание определить операцию возведения в степень. Мы уже по существу определили возведение в целую положительную степень (α^n есть произведение n сомножителей, равных α). Другими словами, если A упорядочено по типу α, то множество A^n последовательностей длины n с элементами из A с обратным лексикографическим порядком (сравнение справа налево) упорядочено по типу α^n.

Следующий шаг — определить α^ω. Первая идея, приходящая в голову — взять множество $A^{\mathbb{N}}$ бесконечных последовательностей и определить на нём полный порядок. Но как его ввести — неясно. Поэтому можно попробовать определить *возведение в степень* индуктивно с помощью следующих соотношений:

$$\alpha^0 = 1;$$
$$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha;$$
$$\alpha^\gamma = \sup\{\alpha^\beta \mid \beta < \gamma\} \text{ для предельного } \gamma \neq 0.$$

Теорема 18 (о трансфинитной рекурсии) гарантирует, что эти соотношения однозначно определяют некоторую операцию над ординалами, которая и называется возведением в степень.

Замечание. Тут опять мы подходим к опасной границе парадоксов и вынуждены выражаться уклончиво. На самом деле теорема о трансфинитной рекурсии говорила об определении функции на вполне упорядоченном множестве, а ординалы не образуют множества — их слишком много. Кроме того, в ней шла речь о функциях со значениями в некотором заданном множестве, которого здесь тоже нет. Подобные индуктивные определения можно корректно обосновать в теории множеств с использованием так называемой *аксиомы*

подстановки, но мы об этом говорить не будем. Вместо этого мы дадим явное описание возведения в степень, свободное от этих проблем.

Чтобы понять смысл возведения в степень, посмотрим, как выглядит ординал α^ω (для некоторого α). Пусть A — множество, упорядоченное по типу α. Ординал α^ω по определению есть точная верхняя грань α^n для натуральных n. Ординал α^n есть порядковый тип множества A^n, упорядоченного в обратном лексикографическом порядке. Чтобы найти точную верхнюю грань, представим множества A^n как начальные отрезки друг друга. Например, A^2 состоит из пар $\langle a_1, a_2\rangle$ и отождествляется с начальным отрезком в A^3, состоящим из троек $\langle a_1, a_2, 0\rangle$. (Здесь 0 — наименьший элемент в A.) Теперь видно, что все множества A^n можно рассматривать как начальные отрезки множества A^∞, состоящего из бесконечных последовательностей $a_0, a_1, \ldots$, элементы которых принадлежат A и в которых лишь конечное число членов отлично от нуля. (Последнее требование делает корректным определение обратного лексикографического порядка — мы находим самую правую позицию, в которой последовательности различаются, и сравниваем их значения в этой позиции.) В объединении эти начальные отрезки дают всё A^∞, так что это множество с описанным порядком имеет тип α^ω.

Аналогичным образом можно описать возведение в произвольную степень.

Пусть A и B — вполне упорядоченные множества, имеющие порядковые типы α и β. Рассмотрим множество $[B \to A]$, состоящее из отображений B в A, имеющих «конечный носитель» (равных минимальному элементу A всюду, за исключением конечного множества). Введём на $[B \to A]$ порядок: если $f_1 \neq f_2$, выберем наибольший элемент $b \in B$, для которого $f_1(b) \neq f_2(b)$ и сравним $f_1(b)$ и $f_2(b)$.

Теорема 40. Указанное правило задаёт полный порядок на множестве $[B \to A]$ и порядковый тип этого множества есть α^β.

$\lhd$ Нам надо проверить, что указанный порядок является полным и что выполнены требования индуктивного определения степени.

Назовём *носителем* элемента $f \in [B \to A]$ множество тех $b \in B$, для которых $f(b) > 0$ (здесь 0 обозначает наименьший элемент множества A). Назовём *рангом* функции f наибольший элемент носителя (по определению носитель конечен, так что наибольший элемент существует). Ранг определён для всех функций, кроме тождественно нулевой, которая является минимальным элементом множества $[B \to A]$. Чем больше ранг функции, тем больше сама функция в

смысле введённого нами порядка.

Пусть порядок на $[B \to A]$ не является полным и $f_0 > f_1 > > f_2 > \ldots$ — убывающая последовательность элементов $[B \to A]$. Все элементы f_i отличны от 0; рассмотрим их ранги. Эти ранги образуют невозрастающую последовательность, поэтому начиная с некоторого места стабилизируются (множество B вполне упорядочено). Отбросим начальный отрезок и будем считать, что с самого начала ранги всех элементов убывающей последовательности одинаковы и равны некоторому b. В соответствии с определением, значения $f_0(b), f_1(b), \ldots$ образуют невозрастающую последовательность, поэтому начиная с некоторого места стабилизируются. Отбросив начальный отрезок, будем считать, что все f_i имеют одинаковый ранг b и одинаковое значение $f_i(b)$. Тогда значения $f_i(b)$ не влияют на сравнения, и потому их можно заменить на 0. Получим убывающую последовательность элементов $[B \to A]$ с рангами меньше b. Чтобы завершить рассуждение, остаётся сослаться на принцип индукции по множеству B.

(Более формально, рассмотрим все бесконечно убывающие последовательности. У каждой из них рассмотрим ранг первого элемента. Рассмотрим те из них, у которых этот ранг минимально возможный; пусть b — это минимальное значение. В любой такой последовательности все элементы имеют ранг b. Из всех таких последовательностей $f_0 > f_1 > \ldots$ выберем ту, у которой значение $f_0(b)$ минимально; все следующие её члены имеют то же значение в точке b (т. е. $f_i(b) = = f_0(b)$). Заменив значение в точке b нулём, получим бесконечную убывающую последовательность из элементов меньшего ранга, что противоречит предположению.)

Теперь покажем, что такое явное определение степени согласовано с индуктивным определением. Для конечных n это очевидно. Пусть $\gamma = \beta + 1$. Каково (явное) определение α^γ? Пусть B упорядочено по типу β. Тогда мы должны добавить к B новый наибольший элемент (обозначим его m) и рассмотреть отображения $B \cup \{m\} \to A$ с конечным носителем. Ясно, что такое отображение задаётся парой, состоящей из его сужения на B (которое может быть произвольным элементом множества $[B \to A]$) и значения на m. При определении порядка мы сначала сравниваем значения на m, а потом сужения на B, то есть полученное множество изоморфно $[B \to A] \times A$, что и требовалось.

Пусть теперь γ — ненулевой предельный ординал и множество C упорядочено по типу γ. Как устроено множество $[C \to A]$? Элемен-

ты, ранг которых меньше $c \in C$, образуют в нём начальный отрезок, и этот начальный отрезок изоморфен $[[0,c) \to A]$. А само множество $[C \to A]$ является объединением этих начальных отрезков (поскольку каждый элемент этого множества имеет конечный носитель) и потому его порядковый тип является точной верхней гранью их порядковых типов, что и требовалось. $\triangleright$

Непосредственным следствием этой теоремы является такое утверждение:

Теорема 41. Если α и β — счётные ординалы, то $\alpha+\beta$, $\alpha\beta$ и α^β счётны.

$\triangleleft$ Для суммы и произведения утверждение очевидно. Для степени: если мы пронумеровали все элементы вполне упорядоченных множеств A и B, то любой элемент множества $[B \to A]$ может быть задан конечным списком натуральных чисел (носитель и значения на элементах носителя), а таких списков счётное число. $\triangleright$

136. Докажите, что $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$ двумя способами: по индукции и с использованием явного определения степени.

137. Докажите, что $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.

138. Докажите, что если $\alpha \geqslant 2$, то $\alpha^\beta \geqslant \alpha\beta$.

139. Докажите, что если $\omega^\gamma = \alpha+\beta$ для некоторых ординалов α, β и γ, то либо $\beta = 0$, либо $\beta = \omega^\gamma$.

140. Какие ординалы нельзя представить в виде суммы двух меньших ординалов?

141. Докажите счётность α^β для счётных α и β, используя индуктивное определение степени.

142. Дан некоторый ординал $\alpha > 1$. Укажите наименьший ординал $\beta > 0$, для которого $\alpha\beta = \beta$. (Указание: что будет, если умножить x на степенной ряд $1 + x + x^2 + x^3 + \ldots$?)

Отметим важную разницу между операцией возведения ординалов в степень и ранее рассмотренными операциями сложения и умножения ординалов. Определяя сумму и произведение ординалов, мы вводили некоторый порядок на сумме и произведении соответствующих множеств (в обычном смысле), здесь же само множество $[B \to A]$ определяется с учётом порядка и отлично от A^B. (В частности, при счётных A и B множество $[B \to A]$ счётно, а A^B — нет.)

Явное описание множества $[B \to A]$ позволяет понять, как устроены его начальные отрезки, то есть какой вид имеют ординалы, меньшие α^β.

Рассмотрим некоторую функцию $f \in [B \to A]$. Пусть она отлична от нуля в точках $b_1 > b_2 > \ldots > b_k$ и принимает в этих точках значения $a_1, a_2, \ldots, a_k$. Нас интересуют все функции, меньшие функции f.

Все они равны нулю в точках, больших b_1. В самой точке b_1 они могут быть либо меньше a_1, либо равны a_1. Любая функция первого типа меньше любой функции второго типа. Функции первого типа могут принимать любые значения в точках, меньших b_1, а в точке b_1 имеют значение из $[0, a_1)$. Тем самым их можно отождествить с элементами множества $[[0, b_1) \to A] \times [0, a_1)$, и при этом отождествлении сохраняется порядок.

Функции второго типа (равные a_1 в точке b_1) снова разбиваются на две категории: те, которые в точке b_2 меньше a_2 и те, которые в b_2 равны a_2. Функции первой категории отождествляются с элементами множества $[[0, b_2) \to A] \times [0, a_2)$. Функции второй категории снова разобьём на части в зависимости от их значения в точке b_3 и т. д. Таким образом, $[0, f)$ как упорядоченное множество изоморфно множеству

$$[[0, b_1) \to A] \times [0, a_1) + [[0, b_2) \to A] \times [0, a_2) + \ldots + \\ + [[0, b_k) \to A] \times [0, a_k).$$

Переходя к ординалам (начальные отрезки — это меньшие ординалы), получаем такое утверждение:

Теорема 42. Всякий ординал, меньший α^β, представляется в виде

$$\alpha^{\beta_1}\alpha_1 + \alpha^{\beta_2}\alpha_2 + \ldots + \alpha^{\beta_k}\alpha_k,$$

где $\beta > \beta_1 > \beta_2 > \ldots > \beta_k$, а $\alpha_1, \alpha_2, \ldots, \alpha_k < \alpha$. Такое представление однозначно и любая сумма указанного вида является ординалом, меньшим α^β.

$\lhd$ Возможность такого представления мы уже доказали. Последнее утверждение следует из того, что любая сумма такого вида является начальным отрезком в множестве $[B \to A]$ (где A и B упорядочены по типам α и β) и разным суммам соответствуют разные начальные отрезки. $\rhd$

Это утверждение обобщает описанную нами ранее (с. 89) «позиционную систему обозначений с основанием α» для ординалов, меньших α^k; теперь вместо k можно использовать любой ординал.

Можно было бы сразу сказать, что элементами $[B \to A]$ являются

формальные суммы вида

$$\alpha^{\beta_1}\alpha_1 + \alpha^{\beta_2}\alpha_2 + \ldots + \alpha^{\beta_k}\alpha_k$$

(где $\beta > \beta_1 > \ldots > \beta_k$ и $\alpha_1, \ldots, \alpha_k < \alpha$) с естественным порядком на них.

Теперь уже понятно, как устроены ординалы в последовательности

$$\omega^\omega, \omega^{(\omega^\omega)}, \ldots$$

Первый из них образован «одноэтажными» выражениями вида

$$\omega^{b_1}a_1 + \omega^{b_2}a_2 + \ldots + \omega^{b_k}a_k,$$

где a_i и b_i — натуральные числа (и $b_1 > \ldots > b_k$). Если в качестве $b_1, \ldots, b_k$ разрешить писать любые «одноэтажные» выражения указанного вида, то полученные «двухэтажные» выражения упорядочены по типу $\omega^{(\omega^\omega)}$. Разрешив в показателях двухэтажные выражения, мы получим трехэтажные выражения, которые образуют следующий ординал и т. д. Если объединить все эти множества, то есть не ограничивать число этажей (которое для каждого выражения тем не менее конечно), то получится множество, упорядоченное по типу

$$\sup(\omega, \omega^\omega, \omega^{(\omega^\omega)}, \ldots)$$

Этот ординал обозначается ε_0.

143. Докажите, что

$$\varepsilon_0 = \omega + \omega^\omega + \omega^{(\omega^\omega)} + \ldots$$

144. Определим для натуральных чисел операцию «тотальной замены основания k на l» (здесь k и l — натуральные числа, причём $l > k$) следующим образом: данное число n запишем в k-ичной системе, то есть разложим по степеням k, показатели степеней снова запишем в k-ичной системе, новые показатели также разложим и т. д. Затем на всех уровнях заменим основание k на основание l и вычислим значение получившегося выражения. Докажите, что начав с любого n и выполняя последовательность операций «вычитание единицы – тотальная замена основания 2 на 3 – вычитание единицы – тотальная замена основания 3 на 4 – вычитание единицы – тотальная замена основания 4 на 5 – ...», мы рано или поздно зайдём в тупик, т. е. получится нуль и вычесть единицу будет нельзя. (Указание: заменим все основания сразу на ординал ω; получится убывающая последовательность ординалов, меньших ε_0.)

2.13. Приложения ординалов

В большинстве случаев рассуждения с использованием трансфинитной индукции и ординалов можно заменить ссылкой на лемму Цорна; при этом рассуждение становится менее наглядным, но формально более простым. Тем не менее бывают ситуации, когда такая замена затруднительна. В этом разделе мы приведём два подобных примера.

Первый из них касается борелевских множеств. (Для простоты мы рассматриваем подмножества действительной прямой.) Семейство подмножеств называется *σ-алгеброй*, если оно замкнуто относительно конечных и счётных пересечений и объединений, а также относительно перехода к дополнению. (Это означает, что вместе с каждым множеством A это семейство содержит его дополнение $\mathbb{R}\setminus A$, и вместе с любыми множествами A_0, A_1, ... семейство содержит их объединение $A_0 \cup A_1 \cup \ldots$ и пересечение $A_0 \cap A_1 \cap \ldots$) Пример: семейство $P(\mathbb{R})$ всех подмножеств прямой, очевидно, является σ-алгеброй.

Теорема 43. Существует наименьшая σ-алгебра, содержащая все отрезки $[a, b]$ на прямой.

$\lhd$ Формально можно рассуждать так: рассмотрим все возможные σ-алгебры, содержащие отрезки. Их пересечение будет σ-алгеброй, и тоже будет содержать все отрезки. (Вообще пересечение любого семейства σ-алгебр будет σ-алгеброй — это очевидное следствие определения.) Эта σ-алгебра и будет искомой. $\rhd$

Множества, входящие в эту наименьшую σ-алгебру, называют *борелевскими*.

145. Докажите, что всякое открытое и всякое замкнутое подмножество прямой является борелевским. (Указание: открытое множество есть объединение содержащихся в нём отрезков с рациональными концами.)

146. Докажите, что прообраз любого борелевского множества при непрерывном отображении является борелевским множеством.

147. Пусть f_0, f_1, ... — последовательность непрерывных функций с действительными аргументами и значениями. Докажите, что множество точек x, в которых последовательность $f_0(x)$, $f_1(x)$, ... имеет предел, является борелевским.

Борелевские множества играют важную роль в *дескриптивной теории множеств*. Но мы хотим лишь продемонстрировать использование трансфинитной индукции (которую трудно заменить на лемму Цорна) на примере следующей теоремы:

Теорема 44. Семейство всех борелевских множеств имеет мощность континуума.

◁ Класс борелевских множеств можно строить постепенно. Начнём с отрезков и дополнений к отрезкам. На следующем шаге рассмотрим всевозможные счётные пересечения и объединения уже построенных множеств (отрезков и дополнений к ним).

148. Докажите, что при этом получатся (среди прочего) все открытые и все замкнутые подмножества прямой.

Далее можно рассмотреть счётные объединения и пересечения уже построенных множеств и т. д.

Более формально, пусть $\mathcal{B}_0$ — семейство множеств, состоящее из всех отрезков и дополнений к ним. Определим $\mathcal{B}_{i+1}$ по индукции как семейство множеств, являющихся счётными объединениями или пересечениями множеств из $\mathcal{B}_i$.

Все семейства $\mathcal{B}_i$ состоят из борелевских множеств (поскольку счётное объединение или пересечение борелевских множеств является борелевским). Исчерпывают ли они все борелевские множества? Вообще говоря, нет: если мы возьмём по одному множеству из каждого класса $\mathcal{B}_i$ для всех $i = 0, 1, 2, \ldots$ и рассмотрим их счётное пересечение, то оно вполне может не принадлежать ни одному из классов. Поэтому мы рассмотрим класс $\mathcal{B}_\omega$, представляющий собой объединение всех $\mathcal{B}_i$ по всем натуральным i, затем $\mathcal{B}_{\omega+1}$, $\mathcal{B}_{\omega+2}$ и т. д. Объединение этой последовательности классов естественно назвать $\mathcal{B}_{\omega 2}$ и продолжить построение.

Дадим формальное определение $\mathcal{B}_\alpha$ для любого ординала α. Это делается с помощью трансфинитной рекурсии. При $\alpha = \beta + 1$ элементами класса $\mathcal{B}_\alpha$ будут счётные объединения и пересечения множеств из класса $\mathcal{B}_\beta$. Если α — предельный ординал, отличный от 0, то класс $\mathcal{B}_\alpha$ представляет собой объединение всех $\mathcal{B}_\beta$ по всем $\beta < \alpha$. (Класс $\mathcal{B}_0$ мы уже определили.)

Из определения следует, что $\mathcal{B}_\alpha \subset \mathcal{B}_\beta$ при $\alpha < \beta$, так что мы получаем возрастающую цепь классов. Каждый класс замкнут относительно перехода к дополнению (для начального класса мы об этом позаботились, далее по индукции). Все классы $\mathcal{B}_\alpha$ содержатся в классе борелевских множеств, так как мы применяем лишь операции счётного объединения и пересечения, относительно которых класс борелевских множеств замкнут.

Возникает вопрос: как далеко нужно продолжать эту конструкцию? Оказывается, что достаточно дойти до первого несчётного ординала.

Пусть $\aleph_1$ — наименьший несчётный ординал. (Это — стандарт-

ное для него обозначение.) Другими словами, $\aleph_1$ есть семейство всех счётных ординалов, упорядоченных отношением $<$ на ординалах.

Лемма. Класс $\mathcal{B}_{\aleph_1}$ замкнут относительно счётных объединений и пересечений и потому содержит все борелевские множества.

Доказательство леммы. Пусть имеется счётная последовательность множеств $B_0, B_1, \ldots$, принадлежащих $\mathcal{B}_{\aleph_1}$. Ординал $\aleph_1$ — предельный, и класс $\mathcal{B}_{\aleph_1}$ является объединением меньших классов. Поэтому каждое из множеств B_i принадлежит какому-то классу $\mathcal{B}_{\alpha_i}$, где α_i — некоторый ординал, меньший $\aleph_1$, т. е. конечный или счётный ординал. Положим $\beta = \sup_i \alpha_i$. Ординал β есть точная верхняя грань счётного числа счётных ординалов и потому счётен. В самом деле, рассмотрим ординалы α_i как начальные отрезки в каком-то большем ординале (например, в $\aleph_1$); их точная верхняя грань будет объединением счётного числа счётных начальных отрезков и потому будет счётным ординалом.

Теперь первое утверждение леммы очевидно: все B_i лежат в $\mathcal{B}_\beta$, а потому их объединение (или пересечение) лежит в $\mathcal{B}_{\beta+1}$ и тем более в $\mathcal{B}_{\aleph_1}$ (поскольку $\beta + 1$ есть счётный ординал и меньше $\aleph_1$).

Таким образом, класс $\mathcal{B}_{\aleph_1}$ является σ-алгеброй, содержащей отрезки, и потому содержит все борелевские множества. Лемма доказана.

Как мы уже отмечали, все классы $\mathcal{B}_\alpha$ состоят из борелевских множеств, так что класс $\mathcal{B}_{\aleph_1}$ совпадает с классом всех борелевских множеств.

Что можно сказать про мощность классов? Класс $\mathcal{B}_0$ имеет мощность континуума (отрезки задаются своими концами). Если класс $\mathcal{B}_\alpha$ имеет мощность континуума, то и следующий класс $\mathcal{B}_{\alpha+1}$ имеет мощность континуума (каждый его элемент задаётся счётной последовательностью элементов предшествующего класса, а $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$). Каждый предельный класс есть объединение предыдущих, и пока мы не выходим за пределы счётных ординалов, объединение это будет счётно, а $\mathfrak{c}\aleph_0 = \mathfrak{c}$, так что мы не выходим за пределы континуума. Наконец, $\mathcal{B}_{\aleph_1}$ есть объединение несчётного числа предыдущих классов (а именно, $\aleph_1$ классов), но так как $\aleph_1 \leqslant \mathfrak{c}$, то $\mathfrak{c}\aleph_1 = \mathfrak{c}$.

Таким образом, класс $\mathcal{B}_{\aleph_1}$, он же класс всех борелевских множеств, имеет мощность континуума. $\triangleright$

Обычно построение борелевских множеств начинается немного иначе. Именно, на нижнем уровне рассматриваются два класса: открытые и замкнутые множества. На следующем уровне находятся классы F_σ (счётные объединения замкнутых множеств) и G_δ (счёт-

ные пересечения открытых множеств). Ещё на уровень выше лежат счётные пересечения множеств из F_σ и счётные объединения множеств из G_δ, и т. д. Такой подход является более естественным с точки зрения топологии, поскольку отрезки на прямой ничем не замечательны. Можно проверить, что разница между таким подходом и нашим определением невелика.

149. Докажите, что пересечение двух F_σ-множеств является F_σ-множеством (и вообще классы F_σ, G_δ, а также классы следующих уровней, замкнуты относительно конечных объединений и пересечений).

150. Докажите, что F_σ- и G_δ-множества лежат в классе $\mathcal{B}_2$ в соответствии с нашей классификацией.

151. Докажите, что всякое множество класса $\mathcal{B}_2$ отличается от некоторого F_σ- или G_δ-множества не более чем на счётное множество.

152. Докажите, что всякое множество класса $\mathcal{B}_3$ является счётным пересечением F_σ-множеств или счётным объединением G_δ-множеств и что аналогичное утверждение верно для более высоких уровней нашей иерархии.

153. Докажите, что существует открытое множество на плоскости, среди вертикальных сечений которого встречаются все открытые подмножества прямой. Докажите, что существует G_δ-множество на плоскости, среди сечений которого встречаются все G_δ-подмножества прямой. Докажите аналогичные утверждения для следующих уровней.

154. Покажите, что существует G_δ-множество, не являющееся F_σ-множеством. Покажите, что существует счётное объединение G_δ-множеств, не являющееся счётным пересечением F_σ-множеств и т. д. (Указание: воспользуйтесь предыдущей задачей.)

Ординалы часто появляются при классификации элементов того или иного множества по «рангам». Например, можно классифицировать элементы фундированного множества.

Теорема 45. Пусть X — фундированное множество. Тогда существует и единственна функция rk, определённая на X и принимающая значения в классе ординалов, для которой

$$\operatorname{rk}(x) = \min\{\alpha \mid \alpha > \operatorname{rk}(y) \text{ для любого } y < x\}$$

(при любом $x \in X$).

$\triangleleft$ Определим множество X_α рекурсией по ординалу α: X_α состоит из всех элементов $x \in X$, для которых все меньшие их (в X) элементы принадлежат X_β с меньшими индексами β:

$$x \in X_\alpha \iff (\forall y < x)\,(\exists \beta < \alpha)\,(y \in X_\beta).$$

Заметим, что здесь (как и в формулировке теоремы) знак $<$ используется в двух разных смыслах: как порядок на X и как порядок на ординалах.

Очевидно, что с ростом α множество X_α растёт (точнее, не убывает). Докажем, что при достаточно большом α множество X_α покрывает всё X. Если это не так, то из $\beta < \gamma$ следует $X_\beta \subsetneq X_\gamma$ (произвольный минимальный элемент, не лежащий в X_β, принадлежит X_γ). Поэтому отображение $\alpha \mapsto X_\alpha$ будет инъекцией, что невозможно (возьмём ординал, по мощности больший $P(X)$; предшествующих ему ординалов уже слишком много).

Теперь определим $\mathrm{rk}(x)$ как минимальное значение α, для которого $x \in X_\alpha$. Если $\mathrm{rk}(x) = \alpha$ и $y < x$, то $\mathrm{rk}(y) < \alpha$. (В самом деле, по определению X_α из $x \in X_\alpha$ и $y < x$ следует, что $y \in X_\beta$ при некотором $\beta < \alpha$.) Наоборот, если для некоторого ординала γ выполнено неравенство $\mathrm{rk}(y) < \gamma$ при всех $y < x$, то $\mathrm{rk}(x) \leqslant \gamma$. В самом деле, тогда любой элемент $y < x$ принадлежит некоторому X_β с $\beta < \gamma$ (положим $\beta = \mathrm{rk}(y)$) и потому $x \in X_\gamma$ и $\mathrm{rk}(x) \leqslant \gamma$.

Итак, построенная нами функция rk обладает требуемым свойством. Единственность доказать совсем легко: если есть две такие функции, рассмотрим минимальную точку в X, на которой они различаются, и сразу же получим противоречие. ▷

В частности, счётные ординалы можно использовать для классификации деревьев, в которых нет бесконечных путей. Мы будем рассматривать *корневые деревья с конечным или счётным ветвлением* (у каждой вершины конечное или счётное число сыновей), в которых нет бесконечной ветви (последовательности вершин, в которых каждая есть сын предыдущей).

Формально такое дерево можно определить как подмножество T множества $\mathbb{N}^*$ конечных последовательностей натуральных чисел, замкнутое относительно взятия префикса (если последовательность принадлежит T, то любой её начальный отрезок принадлежит T). Элементы множества T мы называем *вершинами* дерева; вершина y есть *сын* вершины x, если y получается из x приписыванием справа какого-то одного числа. Вершина y является *потомком* вершины x, если y получается добавлением к x одного или нескольких чисел.

Мы говорим, что в дереве T *нет бесконечной ветви*, если не существует бесконечной последовательности натуральных чисел, все начала которой принадлежат T. В этом случае отношение порядка

$$y < x \iff y \text{ есть потомок } x$$

фундировано и можно применить предыдущую теорему, определив ранги всех вершин дерева T. Ранг его *корня* (последовательности длины 0) и будем называть *рангом дерева.*

Теорема 46. (а) Ранг любого дерева (описанного вида) является счётным ординалом.

(б) Всякий счётный ординал является рангом некоторого дерева.

$\lhd$ (а) Пусть ранг некоторого дерева, то есть ранг его корня, является несчётным ординалом. Тогда ранг одного из сыновей корня также несчётен. (В самом деле, точная верхняя грань счётного множества счётных ординалов является счётным ординалом; это становится ясным, если рассматривать эти ординалы как начальные отрезки большего — тогда точная верхняя грань будет объединением.) У этого сына в свою очередь есть сын несчётного ранга и т. д. Этот процесс не может оборваться, и мы получаем бесконечную ветвь в противоречии с предположением.

(б) Это утверждение доказывается индукцией: пусть α — наименьший счётный ординал, для которого такого дерева нет. Тогда для всех меньших ординалов деревья есть. Возьмём эти деревья и сделаем их поддеревьями с общим корнем (их корни станут сыновьями этого общего корня). Новое дерево также имеет счётное ветвление и ранг его корня равен α. $\rhd$

155. Пусть имеется счётное дерево, не имеющее бесконечных ветвей. Предположим, что в каждом его листе находится отрезок или дополнение до отрезка, а в каждой внутренней вершине стоит знак пересечения или объединения. Как сопоставить такому дереву некоторое борелевское множество? (Указание: покажите, что в каждой вершине можно единственным образом написать некоторое множество, согласованное с пометками.) Покажите, что все борелевские множества могут быть получены таким способом.

Деревья с пометками, рассмотренные в этой задаче, представляют собой как бы бесконечные формулы, составленные из отрезков и дополнений к ним с помощью операций счётного объединения и пересечения (конечные деревья соответствовали бы конечным формулам). Можно условно сказать, что борелевские множества — это множества, выражающиеся с помощью таких формул.

156. Докажите, что семейство борелевских множеств имеет мощность континнума, используя «бесконечные формулы» — размеченные деревья, в которых нет бесконечных ветвей. (Это доказательство обходится без ординалов, трансфинитной индукции и даже леммы Цорна — хотя и использует аксиому выбора.)

В заключение приведём скорее забавный, чем важный, пример использования трансфинитной рекурсии и ординалов.

Теорема 47. Существует множество точек на плоскости, которое пересекается с каждой прямой ровно в двух точках.

Две параллельные прямые почти что удовлетворяют этому требованию (исключением являются лишь параллельные им прямые). Но избавиться от этого исключения не так просто.

$\triangleleft$ Требования к множеству можно сформулировать так: никакие три точки не лежат на одной прямой, но любая прямая пересекает его не менее чем в двух точках.

Будем строить это множество трансфинитной рекурсией. Пусть α — минимальный ординал, имеющий мощность континуума. (Если континуум-гипотеза верна, то он совпадает с $\aleph_1$, но это нам не важно.) Тогда множество всех меньших ординалов можно поставить во взаимно однозначное соответствие с множеством всех прямых на плоскости. Пусть l_β — прямая, соответствующая ординалу $\beta < \alpha$.

Для каждого $\beta < \alpha$ построим множество M_β, в котором никакие три точки не лежат на одной прямой, следующим образом. Объединим все построенные ранее множества M_γ при всех $\gamma < \beta$. Могут ли в этом множестве (обозначим его T) какие-то три точки лежать на одной прямой? Если да, то эти точки берутся из каких-то множеств M_{γ_1}, M_{γ_2}, M_{γ_3}; возьмём наибольший из ординалов γ_1, γ_2, γ_3; в соответствующем множестве будут три точки, лежащие на одной прямой, что противоречит предположению индукции.

Посмотрим, во скольких точках пересекает прямая l_β множество T. Таких точек (по доказанному) не больше двух. Если их ровно две, то всё хорошо и мы новых точек не добавляем, считая, что $M_\beta = T$. Если их меньше, то мы должны добавить новые точки (до двух), но только так, чтобы при этом не образовалось трёх точек, лежащих на одной прямой. Другими словами, нельзя добавлять точки, которые лежат на пересечении l_β с прямыми, проходящими через пары уже имеющихся точек.

Сколько таких прямых (то есть сколько пар уже имеющихся точек)? По построению видно, что все уже имеющиеся точки лежат по две на каждой прямой l_γ при $\gamma < \beta$. (Строго говоря, это следует включить в индуктивное предположение.) Таким образом, множество T по мощности есть $2\beta = \beta$, а пар точек не больше $\beta^2 = \beta < \mathfrak{c}$. Поэтому запрещённые точки составляют лишь малую (по мощности) часть прямой l_β, и можно выбрать две разрешённые точки.

Теперь осталось объединить множества M_β для всех ордина-

лов $\beta < \alpha$ и получить искомое множество. (По условию три точки на одной прямой в нём появиться не могут, а всякая прямая будет рано или поздно рассмотрена и две точки на ней будут обеспечены.) $\triangleright$

157. Найдите ошибку в следующем «опровержении гипотезы континуума»: пусть $\aleph_1 = \mathfrak{c}$. Упорядочим отрезок $[0,1]$ по типу $\aleph_1$. Рассмотрим функцию двух переменных, равную единице на паре (x,y), если $x < y$ (в смысле этого порядка), и нулю в остальных случаях. Тогда при фиксированном x функция $y \mapsto f(x,y)$ равна единице везде, кроме счётного множества, и потому интегрируема и $\int f(x,y)\,dy = 1$ при любом x. С другой стороны, функция $x \mapsto f(x,y)$ равна нулю всюду, кроме счётного множества, так что $\int f(x,y)\,dx = 0$. Получаем противоречие с теоремой Фубини, которая утверждает, что

$$\int_0^1 \left(\int_0^1 f(x,y)\,dy\right)\,dx = \int_0^1 \left(\int f(x,y)\,dx\right)\,dy.$$

Литература

[1] П. С. Александров, *Введение в теорию множеств и общую топологию.* М.: Наука, 1977.

[2] Н. Бурбаки, *Начала математики. Первая часть. Основные структуры анализа. Книга первая. Теория множеств.* Перевод с французского Г. Н. Поварова и Ю. А. Шихановича под редакцией В. А. Успенского. М.: Мир, 1965. 456 с.

[3] Т. Йех, *Теория множеств и метод форсинга.* Перевод с английского В. И. Фуксона под редакцией В. Н. Гришина. М.: Мир, 1973. 150 с.

[4] Георг Кантор, Труды по теории множеств, перевод Ф. А. Медведева и А. П. Юшкевича, издание подготовили А. Н. Колмогоров, Ф. А. Медведев, А. П. Юшкевич, ответственные редакторы А. Н. Колмогоров, А. П. Юшкевич. М.: Наука, 1985. 431 с. (Серия «Классики науки».)

[5] Пол Дж. Коэн, *Теория множеств и континуум-гипотеза.* Перевод с английского А. С. Есенина-Вольпина, М.: Мир, 1969. 347 с.

[6] К. Куратовский, А. Мостовский, *Теория множеств.* Перевод с английского М. И. Кратко под редакцией А. Д. Тайманова. М.: Мир, 1970. 416 с.

[7] И. А. Лавров, Л. Л. Максимова, *Задачи по теории множеств, математической логике и теории алгоритмов.* Издание второе, М.: Наука, 1984. 224 с.

[8] Ю. И. Манин, *Доказуемое и недоказуемое.* М.: Советское радио, 1979. 168 с.

[9] А. Мостовский, *Конструктивные множества и их приложения.* Перевод с английского М. И. Кратко, Н. В. Белякина и М. К. Валиева под редакцией А. Г. Драгалина и А. Д. Тайманова. М.: Мир, 1973. 256 с.

[10] *Справочная книга по математической логике в четырёх частях под редакцией Дж. Барвайса. Часть II. Теория множеств.* Перевод с английского В. Г. Кановея под редакцией В. Н. Гришина. М.: Наука, 1982. 376 с.

[11] А. А. Френкель, И. Бар-Хиллел, *Основания теории множеств.* Перевод с английского Ю. А. Гастева под редакцией А. С. Есенина-Вольпина. М.: Мир, 1966. 556 с.

[12] Ф. Хаусдорф, *Теория множеств.* Под редакцией и с дополнениями П. С. Александрова и А. Н. Колмогорова. М. – Л.: ОНТИ, 1937.

[13] Дж. Шенфилд, *Математическая логика*, перевод с английского И. А. Лаврова и И. А. Мальцева под редакцией Ю. Л. Ершова. М.: Наука, 1975. 528 с.

Предметный указатель

Указатель имён